iGovernment

Prins, J.E.J.; Broeders, D.; Griffioen, H.; Keijzer, A.G.; Keymolen, E.

Publication date:
2011

Document Version
Publisher's PDF, also known as Version of record

WRR

SCIENTIFIC COUNCIL FOR GOVERNMENT POLICY

iGovernment

Corien Prins, Dennis Broeders,
Henk Griffioen, Anne-Greet Keizer
& Esther Keymolen

AMSTERDAM UNIVERSITY PRESS

iGovernment

This book is based on a report that was published by The Netherlands Scientific Council for Government Policy (WRR). According to the Act of Establishment, it is the Council's task to supply, on behalf of government policy, scientifically sound information on developments which may affect society in the long term, and to draw timely attention to likely anomalies and obstacles, to define major policy problems and to indicate policy alternatives.

The Council draws up its own programme of work, after consultation with the Prime Minister, who also takes cognisance of the cabinet's view on the proposed programme.

Lange Vijverberg 4-5
P.O. Box 20004
2500 EA 's-Gravenhage
Tel. +31 70 356 46 00
Fax +31 70 356 46 85
E-mail: info@wrr.nl
Internet: http://www.wrr.nl

WRR

SCIENTIFIC COUNCIL FOR GOVERNMENT POLICY

iGovernment

Corien Prins, Dennis Broeders, Henk Griffioen, Anne-Greet Keizer & Esther Keymolen

Amsterdam University Press, Amsterdam 2011

Front cover illustration: Silo – Strategy. Concept. Design

Cover design: Studio Daniëls, The Hague
Layout: Het Steen Typografie, Maarssen

Translation: Balance Amsterdam / Maastricht

ISBN 978 90 8964 394 0
e-ISBN 978 90 4851 298 0
NUR 759 / 754

CONTENTS

PREFACE

This book offers a new perspective on the future of government digitization. The Dutch version, entitled *iOverheid*, was presented to the Minister of the Interior and Kingdom Relations, Piet Hein Donner, on 15 March 2011. In it, the Scientific Council for Government Policy (*Wetenschappelijke Raad voor het Regeringsbeleid* – WRR), an advisory body to the Dutch Government, makes recommendations on this important issue. The WRR's task is to make proposals, based on broad analysis and scientific insights, for the strategic direction of Dutch policy. To this end, the WRR submits advisory reports to the government on issues which merit special attention. The current English version of the *iOverheid* report draws mainly on material relating to the Dutch situation and developments – in their EU context – but the analysis and the policy perspective provided should prove valuable in other national contexts as well. After all, the Netherlands is by no means unique, neither in the high stakes involved with the success or failure of ICT in government, nor in the sometimes feeble grasp that public authorities seem to have on developments in this field, especially in assessing the wider societal consequences of digitization. The central message that this book puts forward is that political attention needs to be shifted towards the intricacies of the web of information flows that is taking shape, instead of the intricacies of the individual technologies and applications that make these information flows technologically possible. The message that governments should see and act like an iGoverment instead of an eGovernment is a message that is worth testing in different national contexts.

This book was drawn up by a project team headed by Corien Prins, a member of the Scientific Council for Government Policy (WRR). The project team further consisted of the following members: Dennis Broeders (project coordinator), Colette Cuijpers, Henk Griffioen, Anne-Greet Keizer and Esther Keymolen. Mark van Loon, Annemarth Idenburg and Tamara Snijders, and Astrid Souren contributed to the preparatory work.

The book is based on a detailed analysis of the extensive Dutch and international academic literature, research commissioned by the WRR, and meetings and interviews with external experts from varying levels of government, politics and academia. Some of the experts work for ministries or other government bodies (the Office of the National Ombudsman, the Data Protection Authority, the Netherlands Court of Audit, the Council of State); in Parliament (members of the Dutch House of Representatives and the Dutch Senate); government agencies, research institutions (the Rathenau Institute, HEC), Dutch universities, companies and other relevant organisations (ECP-EPN, ICTU, BPR, etc.); in some cases universities abroad; European institutions (the European Commission, the European Parliament and the European Data Protection Supervisor); and the Permanent

Representation of the Netherlands to the EU in Brussels. A list of people interviewed for this report or for one of the preliminary studies is given in one of the appendices. The authors are grateful to all of these individuals for their time, expertise and suggestions, which have been invaluable. The underlying research, which was commissioned by the WRR, was published in two forms. Some of the studies were included as chapters in the background study published simultaneously with the Dutch edition of this book entitled *De staat van informatie* (Broeders, Cuijpers & Prins 2011); the rest were published on the WRR's website in the *iOverheid* series, the first appearing in the autumn of 2010. The Dutch versions of all of these publications can be downloaded from www.wrr.nl. The WRR is grateful to all of the authors and experts for their contribution and for attending the working conferences organised within the context of the preliminary studies.

The project group had the opportunity to discuss at length the preliminary project outcomes and recommendations with a group of international researchers during a seminar organised by the WRR and the Oxford Internet Institute (OII) in May 2010. The WRR would like to thank all those who attended for contributing to that discussion. Special thanks are due to a number of individuals who commented on the draft report in the final phase, or who brainstormed about the project set-up at the start: Krijn van Beek, Arie van Bellen, Alex Brenninkmeijer, Ybo Buruma, Wim van de Donk, Maarten Hillenaar, Ignace Snellen, Stavros Zouridis and Arre Zuurmond. We are most grateful for their assistance.

SUMMARY

The ubiquitous use of ICT in government means that we can no longer label it 'eGovernment', where the focus is on providing services and on utilising technology. What has in fact evolved in everyday practice is closer to 'iGovernment', typified by information flows and data networks and focusing not only on providing services but also on control and care. iGovernment is bringing about far-reaching changes in the relationship between the public and the authorities. Although it has practical – and very real – implications for policy and implementation, iGovernment, with a few rare exceptions, has so far been flying under the political and administrative radar. Based on this observation, this volume argues in favour of making 'iGovernment self-awareness' a key objective. It provides a range of policy and institutional recommendations for making the necessary paradigm shift from eGovernment to iGovernment as smooth as possible.

The impact of ICT on society and government

ICT has become part of the very fabric of government and it increasingly impacts on organisations, the professionals who work there, and their relationship with the public. All of the policy plans for eGovernment – which focus on internal operational issues, the provision of government services, and the technology itself – express massive trust in ICT as an instrument for making government more effective, client-friendly and accessible, for improving the quality of government, and for preparing government for the future. Increasingly, policymakers and politicians are turning eagerly to ICT to assist with the complex administrative work of government and to help them tackle urgent social issues such as terrorism, security, mobility, and the provision of good and affordable care. In addition to public services, other government tasks are rapidly being digitized.

Technology has very nearly become a matter of course in government, whether at the local, national or European level. Technology is 'rolled out', practices are 'streamlined' and services are 'updated'. The level of 'techno-trust' among politicians and policymakers can be seen in the hugely ambitious plans they have made for and with ICT, not only in terms of the technology itself, but also with respect to actual policy. Currently popular policy themes – for example 'customisation' and proactive policy-making – would be unimaginable without the backdrop of digitization. In an effort to map out the future and anticipate what lies ahead, government is utilising and interlinking systems in such areas as security and care. For example, there is now a reference index in the Netherlands for children at risk; European immigration databases are meant to prevent more irregular migrants settling in the Netherlands; and special investigative databases and cross-border exchanges of passenger and bank details are helping to prevent new terrorist attacks worldwide. And it is not only national government that is planning new

systems or calling for more and better information. Whole networks of interlinked systems and information processes are developing between implementing agencies and within local government. Globalization processes are also ensuring that information policy in the Netherlands is taking shape partly within the context of international as well as European applications and systems. There is also constant pressure at these levels to expand the systems' functions, to add more information categories, and to give a growing number of authorities access to the information stored there.

Politicians who wax lyrical about new applications as well as interlinked systems and information flows argue that these will increase security and improve effectiveness and efficiency. Combined with the problem-solving 'image' of ICT, the arguments they offer are more or less self-evident: in each case (a system, a link), these arguments appear to weigh more heavily in the equation than such ideals as transparency, privacy, freedom of choice, or accountability. Many policymakers who 'own' or advocate such applications tend to regard ICT as an instrument, and they assume – and regularly make a point of saying so – that it will not alter the primary process of government. They do not, or only barely, acknowledge or perceive the unintended but very real impact that digitization has on the way government operates, if only because the public in general has itself changed. Although the instrumental dimension of ICT is important, this attitude has led to a certain paucity, in the sense that that there is a virtual absence of any effective form of evaluation. Credible evaluations are rare and there are no sound standards for assessing applications. The debate continues to focus on the security of the technology (e.g. the public transport ID chip card) or the financial debacles (e.g. the various failed ICT projects).

The process of interlinking and sharing data runs parallel to the collapse of partitions between policy areas, between government organisations, and between the public and private sectors. Increasingly, such partitions are regarded – including by the public – as impediments to efficient and effective public administration. The popularity of data-sharing within supply chains and networks – something facilitated by unique ID numbers (the Citizen Service Number) and authenticated records – means that information can easily cross over traditional boundaries, even though the responsibility for the quality and reliability of that data have not evolved at the same pace. Information is disseminated, and it is used and processed by many different public authorities. Government bodies operating in widely diverging areas and with very different objectives are increasingly making use of the same 'pooled' information. But no one knows precisely who is responsible for the information (or its accuracy), and so people must allow for the possibility that 'their' information will come to lead a life of its own in public and private hands.

Politicians and policymakers propagate, discuss and assess all of the trends and developments described above, using a range of different rationales, ideas and normative viewpoints. The best-known of these are efficiency, effectiveness, security, privacy, and transparency. Ultimately, the form in which a new system or new link between information sources is cast is the outcome of a complex dynamic relationship between all of these standards. That outcome concerns not only the technology – which is often the focus of the debate – but in particular its social, administrative and legal implications, which receive much less attention. To clarify this dynamic process and to offer some guidance when it comes to weighing up the various rationales at work, we have divided them into three categories: driving principles (such as security, effectiveness, and efficiency), underpinning principles (privacy and freedom of choice), and process-based principles (transparency and accountability). Driving principles are associated with government's 'drive' to utilise ICT in all kinds of different areas. They are closely bound up with notions of improvement and quality gains. Underpinning principles have to do with guaranteeing rights and freedoms, charting 'silent losses' as the process of digitization proceeds, and protecting the autonomy of the individual. They form a kind of counterbalance to the driving principles. Finally, process-based principles provide the procedural framework that makes a transparent and verifiable comparison between driving and underpinning principles possible.

iGovernment as reality

This volume shows that the nature of government is changing fundamentally, step by step, decision by decision, under the influence of digitization. A *de facto* practice has developed – virtually unnoticed – in which interrelated information flows dominate the character of government. These information flows therefore also determine the new possibilities open to the authorities and the public – as well as their dependencies and vulnerabilities. In everyday life , however, the overall idea of the 'information Government' – *iGovernment* – is virtually the last thing driving the way politicians and policymakers think and work: the vast majority of government initiatives relating to digitization and the information flows they generate are debated, evaluated and introduced in isolation. Individual initiatives are not – or scarcely ever – assessed on the basis of their impact or potential impact on government and society as a whole. The most significant omission is the failure or near-failure to view such initiatives within the context of the fast-expanding and rapidly diversifying information flows. Politicians and policymakers are not aware of iGovernment and, given the unremitting ascendency of ICT, that is certainly a problem.

The accumulation of ad hoc decisions about new technologies, the lack of awareness that iGovernment is on the rise, and the absence of any related discussion mean that when it comes to the development of iGovernment, 'the sky's the limit' – there appear, in effect, to be no limits. No one has restricted the dispersal of indi-

vidual applications or the linking up of information flows, because no one has claimed stewardship of the whole. It no longer seems possible to set a frame of reference for collecting or linking information. The result is that information becomes contaminated, it is unclear who is responsible for information flows, and individuals, businesses and even government organisations become trapped and stifled in the tangle of government data. Questions and concerns regarding the relationships between information flows and their implications are left unaddressed. As a result, not only people but also government itself are vulnerable. The debate among Dutch politicians and policymakers lacks a broader view of iGovernment and a meticulous and verifiable assessment of its driving pr, underpinning and process-based principles.

Although iGovernment is still developing and growing rapidly, and although it has scarcely made any impression on politicians and policymakers, it is already having a very real impact. At the same time, the lack of 'awareness' of the features of iGovernment means that this impact is scarcely taken into account in policymaking, and that politicians and policymakers do not realise sufficiently precisely *what* is developing, let alone *how* they can guide the development process in the right direction. If the Dutch government wants to steer the digitization process in the right direction while leaving enough scope for ICT-driven innovation, it will have to make the transition from eGovernment to iGovernment in thought, word and deed. Government's main challenge – and in fact, the challenge facing all tiers of public administration – is to understand that it has *already* become iGovernment, with all that that implies. Meeting this challenge will require it to shift perspective and develop an appropriate institutional framework. It must also, crucially, leave behind the narrow focus on individual applications, and turn instead to the idea of networked information management. The final requirement is that government must have an open-minded attitude toward trends and developments in the information society (iSociety). iGovernment cannot be structured in isolation. Its motto must therefore be: 'Make sure we involve the iSociety in building an iGovernment that will last'.

Administrative principles for iGovernment

Two issues are of vital importance in making the administrative transition to iGovernment. First of all, the scrupulous development of iGovernment is impossible unless we assess the driving, underpinning and process-based principles with an open mind. In addition, government must exercise particular caution, both in this assessment and in its policymaking and policy implementation, whenever the three processes of information handling noted in this book come into play. These processes – furnished with symbolic warning flags – are associated with a) the networking of information, b) the compiling and enhancing of information, and c) the pursuit of preventive policy based on information.

The three clusters of principles described in this volume – driving, underpinning and process-based – should be well balanced at all decision-making levels. This is no mean task, given that a quasi-quantitative concept such as efficiency, a more normative concept like freedom of choice, and a process-based concept like accountability all clearly fall under different registers of analysis. Nevertheless, if iGovernment is to be evenly balanced, these three clusters of principles must also be thoroughly and properly assessed. They must be clarified, they must be verifiable, and publicly accountable. That does not happen nearly enough yet. Government must explain its rationale publicly at every level, from preparation and introduction of a specific application to the far-reaching diversification of processes and information flows that form the building blocks of iGovernment. It should do so not only at the national level, but also for assessments at the international and, specifically, at the European level. Clarifying the principles and making them as verifiable as possible would raise a number of issues and open them up for discussion. One such issue is the fact that politicians and policymakers are often irrationally optimistic about the potential of ICT. This is often why there impossible deadlines are set and why there are expensive ICT failures. Clarification would also show that spill-over and function creep are often quietly factored into the equation. Real iGovernment self-awareness requires politicians to take the expression 'A government forewarned is a government forearmed' seriously in the digital domain as well, and to apply this expression to implicit but foreseeable ICT trends. Government often anticipates the future in its policymaking, and it would be to its credit to do the same in its political assessments, openly and above board.

Secondly, the transition to iGovernment requires that government become much more aware of various features of information than is now the case. We are referring here to *processes* of information handling and use, specifically because such processes have a huge impact on the nature and reliability of the information that feeds iGovernment. We have therefore tagged three interrelated processes with warning flags: when information is either part of or the result of these processes, government must pay strict attention to the quality of the information and consider who bears responsibility for it. The three processes that we have flagged in this way are:

a The *networking* of information, i.e. shared use and management of information within a network of actors.
b The *compiling* and *enhancing* of information, i.e. creating new information and profiles based on different sources in different contexts.
c Pursuing *preventive* and proactive policy based on information, i.e. actively evaluating and intervening in society based on an information-driven risk calculation.

These three information processes, which are the core of iGovernment, enable it to fine-tune and customise policy, obtain a comprehensive picture of the public

and of the policy issues, and take proactive action where needed. At the same time, they are processes that themselves have an impact on information: they influence its nature, reliability, recognisability, contextuality and traceability. It is important to realise – much more so than is now the case – that it is precisely these three processes that are having the biggest impact on (a) the quality of information *content* and (b) the demands made on the *organisational* context of information flows. The quality and vulnerability of information and information processes therefore require constant, proactive vigilance throughout all branches of national government. We must also have a much greater degree of openness and transparency, so that we can help people understand what information is being collected on them and assist them in correcting it where necessary. Right now, people are almost powerless to correct errors in personal information within the vast iGovernment information networks – errors that sometimes have huge repercussions. Finally, iGovernment's 'memory' demands particular attention. Both the importance of 'forgetting' – people should not be judged eternally on the information that government has stored about them – and of saving and archiving require a radical cultural transition and a firmly grounded strategy.

Limits to the growth of iGovernment

When iGovernment is not self-aware, its natural tendency will be to continue expanding. After all, only self-awareness will induce it to set limits to its own growth. The scrupulous development of iGovernment also means being prepared to set limits to it. Although this book does not define such limits – in essence, that is a political matter – it does indicate where those limits might be found. In the first place, the combined processes of assessing principles and being alert to warning flags force us to consider the limits of iGovernment. Other reasons to set limits may include the mixing of service, care and control, and the diffuse boundaries between public and private information flows. What is also of huge importance is the fact that the Internet has created an entirely new information environment, one from which iGovernment cannot withdraw and within which it is obliged to function. The relationship to this 'world outside' also makes it very important to set well-argued limits.

An institutional agenda for the transition to iGovernment

Prudent efforts to build iGovernment require changes not only in policy but also at the institutional level. A government that has taken on another guise in the digital sense must also make the necessary organisational changes. When government is linked up in terms of its information flows, the accountability structure must fit in with this new reality and operate with the necessary efficiency. 'iGovernment self-awareness' is not just a status to be enjoyed, but rather an ongoing challenge that must ultimately be ingrained in every tier of government. In the short term, however, central government will have to foster that self-awareness. Fleshing out the targets for iGovernment will therefore require an institutional transformation

that assigns and embeds three functions within government:

a The *strategic function*, i.e. guaranteeing the well-considered, ongoing development of iGovernment.
b The *societal function*, i.e. making iGovernment more transparent for citizens and improving its accountability vis-à-vis individuals who become entangled in information networks.
c The *operational function*, i.e. improving the well-reasoned alignment between policy, implementation, technology, information flows and networks. Also, improving the commissioning practices of government.

These three functions constitute the absolute minimum requirements for shaping iGovernment self-awareness and acting on the implications of the new reality. It is no easy matter to map out the institutions associated with these three functions properly, but it is important that these functions are actually entrusted to organisations. The institutional transformation as such is much more important than the precise designations for the institutions proposed in this volume. At the strategic level, we propose a standing committee for iGovernment that investigates and assesses digitization processes in the light of iGovernment as a whole, and that reports to Parliament. At the societal level, we propose setting up an iPlatform in order to concentrate and increase the transparency of iGovernment *vis-à-vis* citizens. Accountability can be entrusted to an iAuthority, responsible for dealing with any problems that citizens encounter with iGovernment (and given the power to take binding decisions). Finally, it is of vital importance at the operational level to ensure professionalism in commissioning practices and to prioritise not technical expertise, but expertise at the interface of technology and policy.

In essence, this publication is about government taking responsibility for the way it uses ICT. But government naturally also has a role to play in the information society. In addition to being accountable for iGovernment, government is responsible to some extent for the way the iSociety functions. What aspects of the information society should government be concerned about, and when should it intervene (and how)? The general public and businesses move ahead, inspired by the promise of new technologies and profits. When this development is not offset against underpinning principles and balanced against the outcome of process-based principles that make information flows transparent for the public – and, if necessary, open to criticism – then those involved iGovernment should at the very least ask whether the time has not come to take action.

PART I

INTRODUCTION AND CONTEXT

1 DIGITIZING THE CITIZEN AND GOVERNMENT

1.1 THE EXISTENTIAL ROLE OF DIGITIZATION

Digitization is a fascinating phenomenon whose impact on society can hardly be overestimated. Many key societal and economic processes have come to rely heavily on ICT systems – systems that are essentially based on infinite series of zeros and ones. These simple digits are capable of converting analogue signals representing texts, images and sounds into digital versions of the same. One noteworthy feature of digitization is the relative ease with which users can gather, store, search, and share information, resulting in an unparalleled range of new products, services and applications. And it can all be done at breakneck speed: a mere mouse click and information available on the Internet can be shared with others on Twitter, Facebook, blogs or other websites. Businesses, public authorities and non-profit organisations fill whole databases, online or otherwise, with data relating to the widest possible variety of subjects, from purchasing behaviour to non-payers and from DNA markers to the fingerprints of the entire population of the Netherlands. Digital information is developing into a universal language that is making the world a much smaller place than it was before. The fact that information is so easy to replicate can even produce global shockwaves, as illustrated by the WikiLeaks affair in late 2010 – described as "the first sustained confrontation between the established order and the culture of the internet" (Naughton 2010b).

The effects of digitization are huge – and extremely varied. WikiLeaks embodies its disruptive power (whether one regards that power in a positive or negative light), but its influence in more 'traditional' contexts, including government, is also enormous. It is no wonder that the public sector is eager to reap the benefits of ICT along with everyone else. An impressive array of digitization projects have been rolled out in recent years in the broad territory covered by government. These are meant to improve government's service delivery and to optimise the way public servants and public services operate – and *co*operate – in government's back office. Changes in service delivery are likely to make the biggest impression on the public. Nowadays, citizens wishing to call on public services can often access them digitally. Almost every local authority allows permit applications and requests for copies of official records to be submitted via its website. Indeed, sometimes that is the only option available. Businesses, for example, are obliged to submit their tax returns electronically. The Dutch government is working hard to set up a general portal, mijn.overheid.nl (i.e. my.government.nl), where citizens can use their personal digital identification code – the 'DigiD' – to log in and transact business directly with government.

Box 1.1 Everyday ICT for citizens

Christine clicks 'send'. She has just applied for a permit to hold a street party that she is organising with some of her neighbours. She did so on her PC, by logging into the local government website using her DigiD number. Being able to submit her application electronically means she won't have to make a trip to the council offices. And while she's already online and has her DigiD log-in code handy, she decides to update the information for her housing and care allowance. She recently started working more hours, and that means that her income has changed. After downloading software from the Tax and Customs Administration website, she gets down to work. Any information already known to Tax and Customs has already been filled in, and that makes things much easier. Once she's completed the form, she sorts through her e-mail inbox. She finds an e-mail from the Education Executive Agency (DUO) informing her that it has recalculated her financial situation, based on her income figures for 2009 as reported by Tax and Customs. If the information in the letter is correct, no action is required on her part and she will shortly be receiving a readjusted repayment schedule for her student loan. There is another e-mail from SISA, a digital information network of youth care organisations. The e-mail tells her that her son Martin's name has been reported to the SISA monitoring system by two various organisations, his school and youth social work agency. The SISA system keeps track of which organisations are monitoring children with potential development problems. Christine is worried and wonders what's wrong with Martin. She rereads the e-mail and the attachment, an information leaflet. She then opens a search engine. She decides to google SISA and see what it all means…

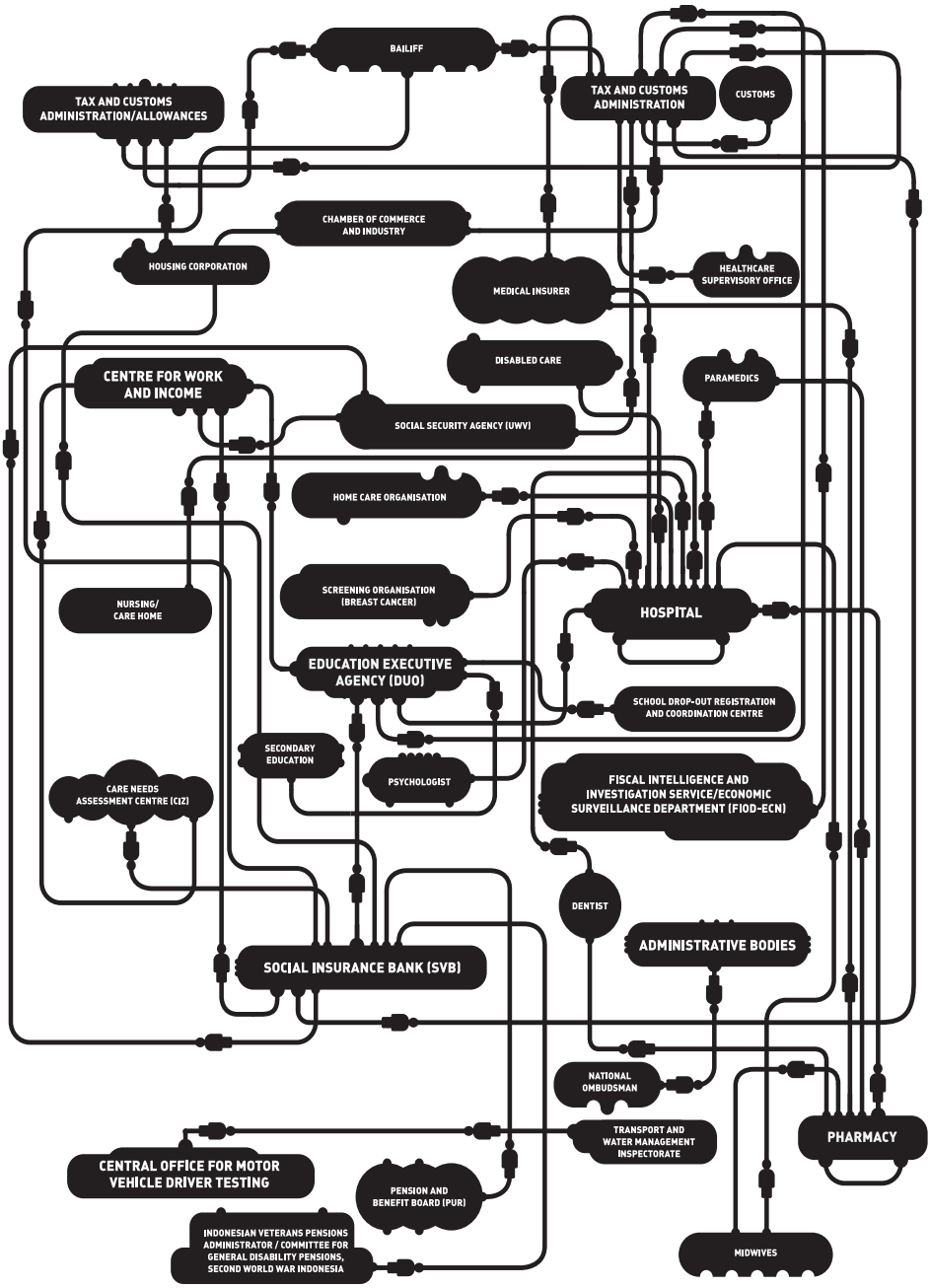
The influence of ICT is also growing fast in other areas in which government bears responsibility, such as healthcare, security, and social insurance. For example, every individual who applies for benefit now has a Digital Client Dossier. The various partners in the benefits supply chain, such as local government, the Social Insurance Bank (SVB) and the Social Security Agency (UWV), use this dossier to share information with one another, so that applicants are only obliged to provide their details once. To prevent errors and enable immediate action in the event of risk, the broader care sector is working on developing an Electronic Patient Dossier (EPD), an Electronic Juvenile Dossier (EJD), and a Reference Index for Juveniles at Risk (VIR). Security and law enforcement officials perform body scans at Schiphol Airport and mount speed cameras along motorways. The Knowledge and Expertise Centre for Intelligent Data Analysis (KECIDA), a department of the Netherlands Forensic Institute, analyses all kinds of information flows (for example on the Internet) in order to assist the police in their enforcement and investigative work. At the same time, the child pornography case uncovered in Amsterdam in December 2010 shows that cross-border data-sharing (in this case, relating to the main suspect's previous conviction in Germany for possession of child pornography) leaves much to be desired. The use of digital applications in public services and the care and security sectors is intended to allow government to discharge its duties more effectively and deliver its services more efficiently. It means that individuals

will have much easier access to government, but also that government will have more records and data on them. In this digital era, government often knows more about the average person than he or she may realise.

Digitization is not limited to the visible interaction between citizens and the authorities. Government is making broad use of ICT 'behind the scenes' as a tool for streamlining work processes and facilitating cooperation between organisations. These changes may not be as evident to the general public as projects highlighted by the media, for example the EPD or the use of body scans at Schiphol Airport, but that does not make them less important. After all, a government that wants to optimise its performance requires streamlined information management. For example, the RINIS Foundation (Institute for the Routing of (Inter)National Information Streams) facilitates the secure and automated exchange of messages between public-sector organisations. RINIS serves as a digital postman; it delivers messages to the right address without knowing what the message says. RINIS affiliates also have access to authentic basic records, for example the Municipal Personal Records Database (GBA), another important component of the authorities' information management system. In fact, these basic records are a dataset containing the data that is most in demand, for example addresses, personal details, company names, and location information. Their purpose is to allow public authorities to use the same basic, reliable data in the course of their work. Another example is the Citizen Service Number (BSN/CSN), which serves as a 'key' for the exchange of personal data. The CSN makes it easier to exchange personal data and makes such exchanges more reliable. In short, government organisations now share data about individuals, allow one another access to information systems, and link up such systems on an everyday basis. Figure 1.1, taken from the Citizen Service Number website, illustrates this point.

The trends described above represent only a fraction of the digitization process taking place in government. It would be virtually impossible to describe all the various projects and initiatives, and not only because there are so many of them, because they are taking place throughout the public sector, or because in many cases the dividing lines between public and private sector are blurred. It is also because they are so dynamic and changeable. The list of projects changes almost constantly under the influence of new technologies, the shifting aims of politicians and policymakers, and the changing needs and expectations of society. An additional factor is that such projects often do not stop at our borders, nor is the Dutch government the only authority involved: europeanization and internationalization play a prominent role here as well. But one thing is certain: digitization has become part of the very fabric of government and increasingly impacts on organisations, the professionals who work there, and their relationship with the public.

Figure 1.1 Data flows between governing and other organisations facilitated by the BSN



Source: www.burgerservicenummer.nl

Now that digital tools have become part of everyday life and are growing more ubiquitous by the day, the fundamental changes they are bringing about and the consequences they have for society and government organisations are becoming clearer. People, businesses and government are reassessing their position in what is rapidly turning into an information society (see Section 1.2). That society is, in essence, a network, and that means that the roles and positions of both the public and the authorities are shifting and changing. It is becoming increasingly clear that these changes are affecting not only the way people and the authorities use information; they also – or should also – have a significant impact on administrative structures and the division of responsibilities. Various authors have already pointed out that digitization will necessitate a transformation of public administration (Frissen 1996; ICT and Government Ad Hoc Advisory Committee 2001; Bekkers, Lips & Zuurmond 2005: 746). What is more difficult, however, is to decide what direction this transformation should take. In addition to the enormous opportunities offered by ICT, it also creates numerous new risks for citizens and government and makes them vulnerable in ways that may not always be apparent.

For example, sharing information electronically may save time and money, but if that data is incorrect, it can be very difficult to remove it from all the interlinked information flows – with everything that implies for the individual in question. A study by the City of Amsterdam some years ago revealed that no less than 7.3 per cent of the addresses in its Municipal Personal Records Database (GBA) contain errors (Advisory Committee on Secure Information Flows 2007: 27). It is not clear whether these errors are 'simply' mistakes, or whether they stem from fraud. In the latter event, it can be very difficult to set the record straight. Witness the much-publicised case of Mr Ron Kowsoleea, a victim of identity fraud. When a criminal passed himself off as Mr Kowsoleea, the latter was flagged as an offender in various police and other government databases. His house was raided, he was arrested at Schiphol Airport, and he received numerous summonses to appear in court. Despite desperate attempts to clear his name, he is still plagued by the identity theft. Kafkaesque circumstances of this kind raise the issue of who is responsible for the correctness of the data in a network of information flows. As regards the police files that caused Mr Kowsoleaa so much distress, it seems that no single authority bore overall responsibility.

People generally seem quite *blasé* about the fact that they now bear a new – often more negative – 'burden of proof' after switching to digital services, whether voluntarily or compulsorily. In addition, new information systems such as the Electronic Juvenile Dossier (EJD) and the Reference Index of Juveniles at Risk (VIR) are by no means neutral digitization initiatives intended solely to improve the efficiency of existing policy or to improve the social safety net. They also influence the relationship between the public and professionals and encroach on

principles such as the privacy and freedom of choice of both parties. At the very least, they cast such principles in a different light. The National Constitutional Committee – which reviewed the Dutch Constitution in the light of globalization and digitization (among other things) at the request of the Government – noted in its report that government is increasingly becoming an electronic government when executing public tasks (Staatscommissie Grondwet 2010: 67). And although the Committee was divided on the need to amend the Constitution in the light of ICT, the tenor of its recommendations is unmistakable: there is every reason for constitutional reformers to get to work, given our changing digital society. The Committee argues that fundamental information rights play a more significant role in the digital age – reason enough to bolster the normative basis of the Constitution and make it more relevant to citizen's lives (Staatscommissie Grondwet 2010: 69).

Digitization also affects the position of government. It comes to depend on systems, making it vulnerable to system malfunctions or even breakdowns, whether it is caused by viruses, cybercrime, faulty maintenance, contaminated or obsolete files, or even the ignorance of users. "Without ICT facilities, we are no longer capable of doing anything. That's how vulnerable and dependent we've become," said Ivo Opstelten, Dutch Minister of Security and Justice, during the Security Conference held on 11 November 2010. But that dependence is also evident in another way: digital government relies heavily on the knowledge and influence of the external consultants, developers, and suppliers who design, implement and maintain the systems.

In short, ICT projects reveal new opportunities, new vulnerabilities, and new risks that determine how the information society is structured and which direction it will take. Such opportunities and risks are what this book is all about. If government organisations 'streamline' information flows and embrace 'chain computerisation' and information networks, what implications will this have for the basic organising principles and accountability structures of public administration? What does digitization mean for the normative precepts that underpin how government executes its tasks? Or, to put it differently: what can people expect from the deployment – often the result of technology push – of ICT by government, and what does that mean for the way government interprets its duties and for its administrative structure? To what extent is the public's growing digital assertiveness putting pressure on the position and role of the public sector? How should we go about striking the right balance between such key values as efficiency, security and privacy?

Before we can investigate and resolve these issues and determine the overall 'fate' of digitization, however, we must decide *who* precisely is responsible for digitization – and that is by no means easy. In fact, ICT seems to be everyone's business

and no one's responsibility these days, whether we mean digitization within the boundaries of government or within society in general. This power vacuum is at odds with government's special position of authority and responsibility. After all, the public interest must be protected in the digital world too, and to do so requires government to take responsibility and to organise its activities accordingly. There is no escaping the dilemma that government faces: while its use of ICT is intended to make people's lives pleasanter and safer, it must at the same time safeguard their fundamental rights and freedoms, such as privacy and autonomy.

1.2 iGOVERNMENT

The quest to resolve this dilemma is the point of departure for this book. Digitization has brought about dramatic changes in both society and government, raising a whole series of vital questions. Many of these touch on the role and responsibility of government. Digitization in government is not taking place in a vacuum; it is a process closely bound up with widespread changes in the information society. ICT, which allows us to gather, share and utilise information in many different domains, is also altering the expectations and responsibilities of both government and citizens. The point is therefore to investigate how ICT has influenced and changed the relationship between government and the people, and the practical and normative implications of that change. Some implications fall into the category 'accepting and adjusting to a new situation', but others necessitate modification at a more fundamental level. The current digitization of society and government, and the unbalanced debate about this process among politicians and policymakers, force us to analyse and assess developments as they unfold. This is not the first time that there has been a call for change, institutional or otherwise; indeed, in some instances – as in the Infodrome project – the appeal has come from a government-initiated programme: "So what we must now do is consider how best to structure the information society" (Infodrome 2001: 165; see also the many advisory reports discussed in Rob 2003). Until now, however, government has not risen to the challenge of developing a political agenda for the information society.

In this book, we conclude that the necessary transition can no longer be put off. Using extensive empirical analysis of government digitization projects (most of them Dutch), we have explored the reality of 'electronic government'. What we have found is that the nature of government is changing dramatically under the influence of digitization. Government not only operates against the backdrop of the information society, it has *itself* become an information government – an *iGovernment*. A *de facto* practice has developed – virtually unnoticed – in which interrelated information flows dominate the character of government. These information flows therefore also determine how government and citizens operate, as well as their dependencies and vulnerabilities. In everyday life, however, the overall idea of iGovernment is virtually the last thing driving the way politicians

and policymakers think and work: the vast majority of government initiatives relating to digitization – the biometric passport or the Electronic Patient Dossier, for example – and the information flows they generate are debated, introduced, and evaluated in isolation. Individual initiatives are hardly ever assessed on the basis of their impact or potential impact on government and society as a whole. There is also a failure or near-failure to view such initiatives within the context of the fast-expanding and rapidly diversifying information flows. iGovernment is not yet part of the mental framework of politicians and policymakers. That is precisely why there are no suitable accountability structures and why we lack the policy instruments to continue the responsible, innovative development of iGovernment. If government wishes to pursue digitization with confidence, it will have to shift the perspective from eGovernment to iGovernment. In line with this challenge, Part III of this book proposes a policy and institutional agenda related to government's networked information management system.

Although this book focuses on iGovernment and therefore deals mainly with the role and responsibilities of government when using ICT in policymaking, its arguments must be considered within the broader setting of the information society. That setting underpins the analysis of how government utilises ICT. After all, what iGovernment can and cannot do and what challenges it faces is determined, at least in part, by the digital dynamics of society. The following section therefore begins by considering a number of crucial trends that are influencing government, the public, their interests and the roles that each plays.

1.3 THE iSOCIETY

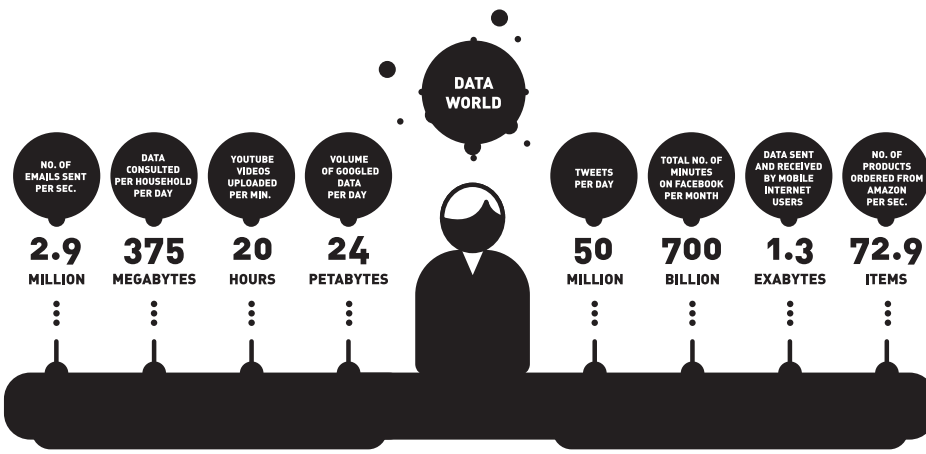
Digitization is bringing about dramatic changes in society without our being able to attribute these changes to any one particular source (Dutton 1999). The many different factors at work are reflected in the typologies used to describe this 'new' society: e.g. the 'information society', the 'network society', and the 'knowledge society'. Although the emphasis varies, all of these labels refer to digitization or ICT and to networks and networked relationships. The impact of ICT on the relationship between government and the citizen is bound up with trends unfolding within the broader setting of the information society (iSociety). For example, starting in the late 1990s, the World Wide Web gradually became the first and most obvious place for many users to search for and disseminate information, but also to create new content, increasingly in collaboration with others. It was precisely for this reason that *Time* magazine selected not a great politician, scientist or artist as its 'Person of the Year' in 2006, but 'YOU' – the group of interactive individuals who were changing the shape of things through the Internet (see also Frissen 2008).

Google, Facebook and Flickr are among the most influential new players that have learned to key into users' desire to search for and share information and interact

with others on the Web. These forces of the new 'information economy' (Van der Laan & De Haan 2005: 13-14) have launched new, innovative digital services and are successful at converting the information collected by these services into annual profits or, at the very least, an attractive stock market value. Thousands of systems architects work behind the scenes to expand the information society, and a similar army of consultants is helping business and government achieve their digitization ambitions. As figure 1.2 illustrates, virtually all of these targets concern the ability to use large quantities of information in innovative ways, either in the public interest or for private purposes. It was already more than a decade ago that Castells (1996) described the network society as an informational capitalist economy, as opposed to the industrial capitalist economy that preceded it.

These trends have naturally also affected government. The increasing capacity of ICT to permit quick and easy information-sharing holds out the promise of more effective and efficient government operations. By the end of the twentieth century, academics and policymakers were discussing the possibility of using ICT to make government more efficient, effective and client-friendly (Boersma et al. 2009; Dunleavy et al. 2006; Van de Donk & Van Dael 2005). Government authorities saw ICT as the pre-eminent channel for achieving innovation. This idea quickly became known as 'electronic government' (eGovernment). It was adopted by governments across the globe, although different countries emphasised different aspects and have arrived at different results (Lenk & Traunmüller 2007; Dunleavy et al. 2006; Mayer-Schönberger & Lazer 2007; Boersma et al. 2009; Prins 2007).

Figure 1.2 Information flows in iSociety



Based on data provided by Cisco, Comscore, Mapreduce, Radicatie Group, Twitter, YouTube.
Source: *Good Magazine*/Oliver Munday/IBM

In the iSociety, digitization is used to innovate and improve processes and relationships in both the public and the private sector. But the use of information and technology has not only intended effects, but also unintended ones. The introduction of ICT often has a far-reaching and unforeseen impact that has not been thought out in advance. This section considers some of the key features of the iSociety, specifically: the innovative power of ICT; the social impact of ICT, which changes relationships; opportunities and risks with respect to security; and the vulnerabilities inherent in digital trails. These factors taken together form much of the background against which iGovernment has developed and will continue to develop.

Innovating and improving: the innovative power of ICT

ICT did not suddenly appear full blown in everyday life. Human progress has always been intimately bound up with advancement of technology. Our ability to get technology to work for us (whether we are talking about 'simple' tools or complex artificial intelligence) has always been a decisive factor in human development. Our wish to control the world around us, combined with our enormous trust in technology as a tool for doing so, often leads us to regard ICT as the ultimate solution to all kinds of social and societal problems. Indeed, we *expect* technology to be used in this way (De Haan 2004). For example, when our security is at stake, we respond with security cameras, biometric access controls, and high-tech defensive weapons. When the issue is efficiency, we migrate services to the Web so that assistance is available 24 hours a day, and rig up databases in a way that makes it easy to collect, combine and then share data.

Businesses were the first to recognise the potential of ICT (De Haan et al. 2005). Influenced by trends in the private sector and the promise of greater effectiveness and efficiency, government too began to experiment with digitization in the 1990s. The transition to electronic government was presented as not only desirable but also unavoidable: "A robust society with a healthy economy requires strong government that uses the most advanced 'tools' available to do its work" (Ministerie van BZK 1998: 3). Efforts to transform government into electronic government converged with two trends that came to dominate the thinking about government and the public sector in the late 1980s (Bekkers & Zouridis 1999; Fountain 2001). To begin with, the financial strains of the rapidly expanding welfare state led to public administration increasingly being regarded as a 'business' (Noordegraaf et al. 1995). In this 'New Public Management' approach, public managers, operational tools, efficiency and service delivery all play a major role in public administration. Secondly, there was a shift in focus: instead of government being viewed as a coordinator, organiser and facilitator, it increasingly came to be seen as an active party (Bekkers & Homburg 2009). In the early days of eGovernment, the primary aim was to lower the threshold to government, improve the quality of its service delivery, and increase the efficiency of its internal processes

(Ministerie van BZK 1998; Ministerie van Economische Zaken 1999). Very quickly, however, trendsetters – such as Denmark, Norway, Sweden, the United States, but also the Netherlands – took things a step further by investing in an integrated back office intended to support not only more efficient but also proactive service delivery. The title of the United Nations' eGovernment Survey 2008, *From EGovernment to Connected Governance* (2009), illustrates this trend. The report claims that "[a] key element of connected governance is the ICT-enabled ability to respond instantaneously with information from across several government agencies, multiplying manifold the government's ability to respond to crisis" (United Nations 2009: 8).

In other words, better service delivery initially meant more efficient service delivery, in keeping with the New Public Management approach. Government was to act as a producer of services for its citizens to consume (Fountain 2001) and would measure its progress by means of quantitative targets: a specified percentage of all services had to be provided by electronic means (Bekkers 2001). That is why in the early days of eGovernment, policymakers and policy documents referred mainly to services delivered *by* government *to* citizens. But the rise of social networking and the growing significance of the iSociety are shifting the focus of government toward public participation and co-creation. Citizens are not just consumers; they can be producers, too.

Online participation: the social impact of ICT

The Internet has become routine in the Netherlands. Statistics Netherlands reports that almost 12 million people (out of a population of 16.5 million) make regular use of the Internet (CBS 2009a). The Dutch are at the top of the EU rankings in both computer ownership and Internet access. In 2009, 93 per cent of the Dutch population had a home computer, and almost eight out of ten people had an Internet connection at home (CBS 2009a). The digital divide between users and non-users has shifted from access to skills. Skills – which can be broken down into technical, formal, strategic and information skills (Van Deursen & Van Dijk 2010) – are especially relevant when consumers also become producers.

The shift from consumption to production is typical of 'Web 2.0', in which individuals use various Internet tools and mobile media to collaborate or 'co-create' content. People maintain social networks, share their expertise and ideas, or work together on projects (for example Wikipedia, the online encyclopaedia) without any of this being centrally organised or controlled. Because popular Web 2.0 applications such as LinkedIn and interactive games do not require extra software to be installed (the Internet serves as their platform), the new services and applications have a very low threshold and are accessible for large numbers of users. It was the arrival of interactive features that made the 'social Web' possible, and online social networks are growing increasingly popular – witness the fact that one in four

people who surf the Internet has a Facebook account and has visited that account at some point in the past month (Facebook 2010). Right now, more than 500 million people are on Facebook. The Dutch counterpart, Hyves, is also popular, with 10.2 million accounts in June 2010 (Hyves 2010).

The more popular social networking sites such as Hyves and Facebook become, the more people are induced to use them. In effect, their popularity dictates the technology that both veterans and novices will end up using (Mulder 2006: 115). After all, it only makes sense to create a profile on Hyves or Facebook if there are others there to interact with. Change has never come about simply because a new technology became available (Van der Laan & De Haan 2005: 13). Designers, companies and producers can create as many elegant applications as they please, but it is users who decide whether their product is useful and convenient and who will make or break it.

The popularity of the Internet is indisputable, but some subtle distinctions should be made when it comes to the 'social Web'. Not everyone who surfs the Web is active on it to the same extent. One third of Internet users limit themselves to reading blogs, watching videos on YouTube, or visiting websites such as Wikipedia (Frissen et al. 2008). About ten per cent of Internet users provide feedback, for example by commenting on online news items or writing book reviews for Amazon.com. Another ten per cent share information, such as photographs on Flickr or music on MySpace. But only three per cent of Internet users actually create content themselves, for example by blogging or writing Wikipedia articles (Frissen et al. 2008). There are also people who deliberately choose *not* to be users, either because they lack the time or inclination, do not trust the relevant application, or simply do not find it useful (Van Dijk 2007; Van den Berg 2008; Wyatt 2005).

Another distinction is related to the idea that the Web is an open forum which everyone can join (Zittrain 2008; Anderson & Wolff 2010). There is now a movement away from the open Web toward various semi-restricted platforms such as Facebook and LinkedIn. Instead of searching the entire Web, users simply go straight to a trusted, familiar website. The rise of mobile devices such as smartphones, iPhones and iPads has encouraged this search strategy: their use of icons makes it very easy to consult a specified source straightaway. The feature that makes these platforms so appealing to users – the ease with which they can share information and interact with others – is also why the companies that founded them are so successful. Restricted systems are simply easier to control than unrestricted ones, and that makes them a more reliable investment (Zittrain 2008). Information from users and about users is the raw material of their business. Their ability to collect, enhance, exploit and also sell large quantities of information allows for personalised advertising and services (Lips et al. 2005).

Digital relationships: ICT causes shifts in positions

The rise of Web 2.0 and the associated influence of the 'crowd' are also affecting what government does (Frissen et al. 2008). Various government departments and agencies want to harness the potential of citizen engagement, sometimes referred to as e-participation. Because the Web makes communication and co-creation possible, government can potentially do much more than merely inform its citizens. The Web also allows for reciprocity between mobilisation, encouragement, creativity and engagement (Bekkers & Thaens 2002; Bekkers & Meijer 2010). For government, the Web may be the key to identifying a new role appropriate to the "fragmentation of society resulting from the ongoing process of differentiation, specialisation and professionalisation" (Bekkers & Meijer 2010: 9). The search for new ways to communicate with the public is one response to the 'gap thinking' that has increasingly come to dominate the discourse about government's legitimacy (see Andeweg & Van Gunsteren 1994; Tiemeijer 2006; Van Gunsteren 2006; Chavannes 2009; Verhoeven 2009; Rob 2010a). The presumed gap between 'government' and 'the citizen' – said to be indicated by a distrust of politics, low voter turnout figures, and dissatisfaction with politicians – raises questions about government's legitimacy in tackling the challenges facing society. ICT is regarded as an ideal means of turning the tide, with e-participation strengthening the legitimacy of politicians and policymakers.

Although the Netherlands ranks among the top five in the world when it comes to eGovernment and shares fifteenth place with France with respect to e-participation (United Nations 2010), it could do more. There is room for improvement in the way government shares information (for example by publishing policy documents), consults citizens (for example about legislation), and allows them to participate in decision-making (United Nations 2010). Another possibility – as yet unexplored – is for government to forge a new kind of relationship with its citizens, one in which politicians and policymakers do not simply take decisions based on a popular mandate, but allow discerning individuals to participate directly in policymaking and decision-making processes.

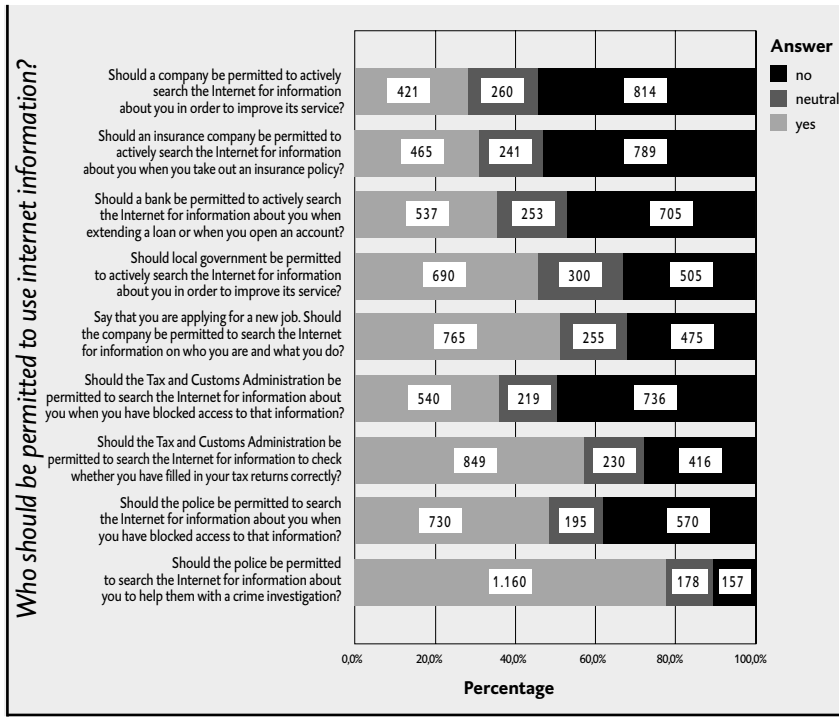
The opportunities that ICT holds out for more public participation and co-creation can also be problematical for government, however. Changes in the roles and positions of various parties are forcing the public authorities to consider their response. The Internet makes it possible for citizens to supervise government and act as a 'countervailing power' in the public arena (Meijer 2004). For example, a vanguard of Web-savvy citizens – in the Netherlands clustered into groups with names such as The New Way of Voting, Bits of Freedom, PrivacyFirst, NLNet, and Internet Society – are lobbying for transparent government. This new generation wants to harness the power of the Web, for example to check on how their elected representatives vote on issues. And if government does not provide the transparency they are seeking, they will organise themselves into groups that will and

set up websites such as 'watstemtmijnraad.nl',[1] which reveals how municipal councillors vote. Besides groups working to foster digital maturity in government, there are other organisations such as Burgerlink ('Citizen Link') that point out the negative implications of the digital imperative. These organisations want to guarantee the public's freedom of choice by keeping other – more traditional – channels of communication with government open alongside the rapidly advancing digital ones.

The Netherlands is not the only country in which a growing number of organisations are demanding more critical reflection on the scope and implications of digitization for society and, in particular, for government. Indeed, a quick survey of other countries, for example Germany or the United States, reveals much livelier and more critical public debate of this issue. Those encouraging such debate in the Netherlands do not in fact receive much public support. That is partly because the Dutch trust the way their government uses ICT. A survey by the Scientific Council for Government Policy (WRR), conducted in cooperation with the ECP-EPN Platform for the Information Society and Centerdata research institute, reveals that the Dutch public places a great deal of trust in the way in which the public authorities use ICT and deal with information. For example, respondents allow government (crime investigation services, the Tax and Customs Administration) much more leeway to use data than business and industry (Attema & De Nood 2010: 2). More than 60 per cent favour digital records in general, and almost 80 per cent support the use of digital records in healthcare. Only ten per cent of respondents are specifically against digital records (Attema & De Nood 2010: 3).

The Dutch attitude contrasts starkly with that in Germany, where citizens have gone to court over the EU obligation to retain communications traffic data and sent masses of angry e-mails to the European Ombudsman after reports surfaced of a new surveillance system, Enfopol. In the United States, private organisations (for example EPIC and the Electronic Frontier Foundation) and individuals have also pressured public authorities to be more transparent. One recent example relates to the ACTA negotiations, a controversial plan to combat Internet piracy. The public's concerns have not fallen on deaf ears, as illustrated by the federal Open Government[2] initiative announced by President Barack Obama almost immediately after his inauguration. Open Data projects are also being launched in the United Kingdom.[3] In Europe, transparency is regarded as a requirement for participatory democracy in an information society and as a prerequisite for legitimate action on the part of government (European Commission 2001). In keeping with this idea, the documents produced by the European Institutions are made available online and European citizens are encouraged to participate in legislative processes. Lor and Britz (2007) argue that freedom of access is vital to facilitating citizen participation in a world in which information plays such a crucial role. Freedom of access

Figure 1.3 Opinions on the use of information in the public and private sectors



Source: Attema & De Nood 2010: 3

to information is sometimes referred to as the 'right to information', and its influence can be seen in countless laws, both national and international (see Singh 2007; Horsley 2007). Government in the Netherlands is also – albeit with some reluctance – allowing citizens to be more closely involved in policymaking. There is, for example, an initiative encouraging public consultation about legislation on the Internet.[4]

Digital trails: the paradox of security and vulnerability

As people exchange and share more and more information electronically, they leave more and longer digital trails. The fact that information flows are becoming an increasingly important factor in what businesses and the authorities do also has implications for the behaviour of individuals and the digital trails they leave behind. Surveillance, data mining, and profiling are modern technical applications that use digital trails to track people and trends and to investigate high-risk (or potentially high-risk) situations or people (House of Lords 2009). The ultimate information society is a transparent society (Tsoukas 1997) and offers ample opportunity to develop 'information-driven policy'. However, it also makes both

citizens and governments more vulnerable (being unfairly treated as a suspect; mistakenly relying on statistical 'certainties').

The claim that technology and information can improve the effectiveness and efficiency of government is not limited to the realm of service delivery. ICT is also increasingly being advocated and deployed in connection with public safety and security issues. The terrorist attacks in New York, Madrid and London have aggravated fears and spurred politicians to put national security and counter-terrorism at the top of the national and international political agenda (Lyon 2003; Edwards & Meyer 2008). Many of the key weapons of counter-terrorism have been made possible by new technology, for example biometrics, data analysis, and information storage and sharing. New organisations have been set up to take charge of implementation, or existing intelligence agencies merged with respect to their information resources. Whereas the United States decided on an institutional approach by setting up the Department of Homeland Security, Europe opted to have its various intelligence services share as much information as possible (Müller-Wille 2008). In addition to these more systematic responses to the threat of terrorism, various incidents have led to a range of ad hoc security measures. For example, after MI 5 uncovered plans to carry out terrorist attacks with liquid bombs in 2006 and a Nigerian man (dubbed the 'underwear bomber') attempted to blow up a plane en route from Amsterdam to Detroit on 25 December 2009, unsealed containers of liquid were banned from all carry-on luggage and total body scans were introduced at Schiphol Airport (Van Eeten 2011). Paradoxically, technical innovation gives both terrorists and politicians tools for action, albeit with diametrically opposed intentions.

Information is a key weapon in international security efforts, leading in the past decade to a boom in data mining, profiling and electronic databases (Lyon 2003; Advisory Committee on Secure Information Flows 2007; Müller-Wille 2008; Balzacq 2008). The clever deployment of information and technology is considered a key factor in a successful security policy, not only on a global level, but closer to home as well – indeed, even *inside* the home. There are a whole battery of applications – camera surveillance, face recognition software on public transport, metal detectors in clubs and bars, biometric fingerprints in passports, the Electronic Juvenile Dossier, the Reference Index for Juveniles at Risk – and many of them have met with public approval. A report by the Netherlands Institute for Social Research (SCP) in 2004 showed that more than 85 per cent of Dutch people approved of the use of security cameras, and close to 100 per cent agreed that DNA research should be applied more broadly to help identify criminals. A more recent study by the Rathenau Institute, ECP.NL and the Dutch Consumers' Association (Rathenau Institute et al. 2007) reveals that the Dutch support the use of digital personal details by crime investigation agencies. More than half (56 per cent) are in favour of retaining digitized copies of passport photographs for crime investiga-

tion purposes (26% are against, and 18% are undecided). Even more recently, a similar survey question relating to fingerprinting produced an even higher approval rating: 66 per cent were for, twenty per cent against and fourteen per cent undecided (Van 't Hof et al. 2010: 93).

But, also apart from counter-terrorism and crime control, security and safety are popular public and political issues in modern Western society, for example in such areas as healthcare, traffic management and environmental protection. Surveys show that safety – or more specifically, the lack of it – rank among the public's top concerns (CBS 2009b), and that government's involvement in issues related to safety – physical safety, social safety nets and international security – has gradually increased, resulting in expanding budgets, a growing regulatory burden, and mounting implementation and coordination problems (WRR 2008b). Government increasingly sees it as its task to actively promote safety by avoiding risk and taking action in such areas as youth care (Prins 2009; Schinkel 2009; Keymolen & Prins 2011), healthcare (Keizer 2011; Pluut 2010) and traffic management (Potters & De Vreeze 2010). Frissen (2009) observes that government's intervention in such areas as public order and safety, youth care, child-rearing, and integration reveals an underlying ideology of the 'makeable society' (a Dutch version of social engineering), expressed in a unique combination of prevention and repression. In terms of its aims, scope and pretensions, policy is becoming more 'total' and all-encompassing (see also Van Gunsteren 2004).[5]

Technology is used to manage and control risk and to avoid damage and injury in the longer term. Beck (1992) has argued that the more a society can harness technology to avoid risk, the less its members are willing to accept that things can sometimes go wrong – a phenomenon that he terms the 'risk society'. The need for control and safety – including social safety nets – has increased in part because hierarchical structures are giving way to network structures. That need is related to processes of decentralisation and privatisation in which responsibilities are divided between numerous organisations and institutions. In an effort to manage and control risk, modern society has become enthralled by the 'safety' philosophy. Boutellier (2004: 44) refers to a 'safety utopia', the "… unattainable pursuit of an optimum link between vitality and safety. The risk society has produced its own utopia, i.e. the union of two opposing needs: the need for freedom and the need for safety." The desire to unite these two needs is confirmed, time and again, by unforeseen events and how the media and politicians respond to them (Van Eeten 2011).

Technology, and ICT in particular, not only makes enforcement and control possible, however – it also facilitates new types of crime and introduces entirely new vulnerabilities into society. Cybercrime, phishing, credit-card fraud, identity theft: these are all crimes that first arose with the arrival of digitization. The UK's

Crime Prevention Panel refers to the 'digitization of crime' (SCP 2004: 475). Govcert (2010), the government organisation that monitors Internet security in the Netherlands, reports in its 2009 Annual Review that cybercrime is growing rapidly. One important reason is that people are now using the Internet for all kinds of everyday transactions (ordering supplies, paying bills), making cybercrime more and more lucrative. The report *Verkenning Cybercrime in Nederland 2009* (Foresight Study of Cyber Crime in the Netherlands 2009) considers five different types of cybercrime (hacking, e-fraud, cyber extortion, child pornography, and hate-mongering) and concludes that cybercrime is 'the people's crime'. Although the media, fiction and even policy documents attribute cybercrime to high-tech, organised criminals, a review of 665 police files reveals that, in fact, many of the crimes are 'petty' ones committed by more or less small-time suspects who operate on their own (Leukfeldt et al. 2010). And it is not only individuals who are increasingly vulnerable to cybercrime. The AIVD – the Netherlands' intelligence agency – warns that government itself is increasingly the victim of digital crime and espionage (2010a; 2010b). Some of the experts interviewed for this publication have commented that government pays only scant attention to this problem and is therefore too little aware of its own vulnerability.[6]

People often have themselves to blame for the new vulnerabilities. Profiles on social networking sites regularly provide personal details, and users are not always aware of who is privy to what information (Boyd 2008). Legal and illegal software, for example spyware, can keep track of the websites a computer user visits and which links he or she clicks on. Private and public-sector organisations contract experts to analyse website visitor behaviour. A great deal of the information gathered through the Internet is also sold, for example to facilitate personalised advertising and services. Users not only leave digital trails on the Internet, however. Their behaviour and actions can also be traced through their mobile phones, in-car navigation systems, digital ID cards and key cards, and even via the signals emitted by the tiny chips now found in all kinds of consumer items such as clothing (radio-frequency identification devices, RFID) (Van Est et al. 2007; Van 't Hof et al. 2010). For example, the Netherlands' public transport chip card has been designed not only as a ticket purchase system but also to enable understanding and management of passenger flows. The card records and analyses travel data and passes that information to others involved in the chip card system: the transport companies, the intermediary system Trans Link, the public authorities, and the passengers themselves (Van 't Hof et al. 2010; Griffioen 2011).

It will be clear that all of these trends and developments raise questions about privacy, safety, security and transparency. Google and Facebook regularly make headlines on the subject of infringements of privacy (Olsthoorn 2010). For example, the Australian police are probing Google Inc.'s Street View mapping service for possible breaches of data-security laws (*Trouw* 2010). Facebook is under fire

because it regularly alters its privacy settings and, in doing so, automatically changes users' default settings to share more information, instead of allowing them to manage it for themselves. Legal battles and bad press have forced these Internet pioneers to reverse certain changes relating to privacy, but it remains difficult, if not impossible, for users to discover which trails they have left behind and what precisely is being done with their information.

1.4 AIM

Given the background of the information society described above, the aim of this book is to offer recommendations for a more self-aware information government (which we call iGovernment). ICT and digitization in the Netherlands have certainly been discussed before, but the impact of many trends identified earlier has now become much clearer. In 1998, for example, ICT was largely "still in its infancy" (WRR 1998: 33). At that time, a mere eight per cent of Dutch people had a mobile phone – a percentage that was expected to increase (WRR 1998: 20). Not only did it do so (by 2009 there were 125 mobile telephone connections per 100 inhabitants in the Netherlands (TNO 2009)), but the enormous number of new functions and apps has fuelled the growth of mobile telephony to unanticipated levels. Today, we use our mobile phones not just to make phone calls, but also to send and receive e-mails, to Twitter, to share files, to watch TV programmes, to take and share photographs, to plan a journey, and to pay for parking. These earlier reports predicted future developments, but now young people are growing up as 'digital natives', never having experienced a world without the Web or mobile phones (Palfrey & Gasser 2008). The fact that our society is becoming progressively more digitized, and that digitization is now virtually the norm, has also affected government and changed its situation considerably, as Part II of this book makes clear.

Anyone following the discourse about digitization today will find that two conflicting 'moods' prevail. On the one hand, policy plans, reports and parliamentary documents support government's efforts and ambitions by enthusiastically explaining what returns digitization can bring: a safe society in which risks are detected in good time, and a more efficient government that delivers tailor-made services to its citizens and that welcomes their input. On the other hand, the debate – particularly in academic and social forums – is often quite negative. Commentators worry about infringements of privacy, the millions of euros wasted on failed ICT projects, expectations that have not been met, new risks such as identity fraud, and insufficiently secure systems and information. Proponents and opponents jockey for position in reports and policy documents and in national and international academic publications. Most striking is that commentators tend to size up developments from one particular perspective (for example: how to narrow the gap between government and citizens through interactive decision-making; how to improve safety; how to avoid the risks posed to privacy and security; and so on).

Many of them also implicitly assume that government has a single consistent vision underpinning its digitization projects. In practice, that is not the case. Government digitization projects and programmes are not the result of some 'grand design'. They are, almost by definition, an arena for public and private parties, ranging from local and administrative authorities to developers, consultants, users, and the general public. Each of these influences the final result. In addition, ICT applications can have unanticipated practical implications and an unexpected impact on the relationship between the various stakeholders and how they deal with responsibilities.

In an attempt to rise above the current discourse, this book surveys the broader forces that information and technology bring to bear on the relationship between government and the citizen. The empirical analysis presented in Part II is the result of a number of choices. Briefly, these choices mean that the book focuses on (1) information as a more important factor than technology, (2) the relationship between government and the citizen, (3) an empirical analysis of the stakeholders involved in information and technology, (4) the dynamics of such principles as security, privacy and transparency, which steer the discussion of digitization projects and determine their evolution, (5) recommendations on the role and responsibility of government. These points are discussed briefly below, with a more detailed explanation in Chapter 2.

The first point is that this book does not concentrate on technological advances *per se*, but instead aims to understand information *processes* (Van de Donk 1997: 153). It analyses information processes whose nature, scope and impact have changed, are changing, or may change under the influence of modern technology. In other words, the focus is not primarily on new ICT applications and technologies such as biometrics and RFID chips, but rather in the impact that they have on the processes of creating, gathering and using information.

Secondly, the book focuses on the relationship between government and the citizen. That does not mean, however, that it ignores other relationships, for example between government and developers, between businesses and consumers, or between various groups of citizens. These relationships are included in the analysis in so far as they influence and help alter the way technology and information are used in the relationship between government and the citizen. Neither end of the government-citizen spectrum is uniform, of course. The labels 'citizen' and 'government' are nothing more than constructs allowing us to consider how actual citizens and actual public bodies relate to one another and to other players. In our empirical analysis, 'government' is broken down into various government bodies and public or semi-public organisations, and 'the citizen' assumes many different guises (and plays many different roles): patient, insured person, juvenile, juvenile delinquent, parent, etc.

Thirdly, in order to fully understand how digitization processes affect the relationship between government and the citizen, we must first understand the dynamic relationship between those involved in digitization. In empirical terms, this means looking beyond the 'paper reality' of legislation and policy documents. The 'real-world' consequences of the biometric passport, the Electronic Patient Dossier and the EU's many plans and databases are what shapes the relationship between government and the citizen. Those involved in that reality – from policymakers and politicians to consultants and developers and finally to end users – together set the digitization agenda and its outcome, but they are seldom themselves the subjects of study.

In the fourth place, our empirical research strategy leads us to consider how the various values vying for precedence – including, but not limited to, privacy and security – are weighed up. What role do they play in development projects, and which parties advocate what fundamental principles, using which arguments? An additional factor is that new circumstances, opinions and options can alter the way politicians and society interpret these principles over time.

Finally, this book makes recommendations for government's responsibilities with respect to the digitization of society and government itself. Technology does not decide every issue; the authorities, developers, users, and the public also help determine whether and how certain technologies come into play. The question then is what specific responsibilities the various parties can be expected to bear. This book focuses in particular on the role and responsibility of government in the information society. In the first instance, that means exploring the responsibility of government when it makes use of ICT in policy implementation. In what way does utilising ICT change the responsibility of government, and how can that responsibility – in particular toward the citizen – be institutionalised?

1.5 METHODS AND STRUCTURE

This book is based on a variety of sources. In addition to Dutch and international academic publications, it is also based on original research, conducted along two different lines. The first consisted of a long series of interviews with experts, policymakers and policy officials, all of inestimable value for the writing of this book. The second consisted of studies and surveys that we carried out ourselves or contracted out to others. This led to a long list of essays and empirical studies published in various forms (on the Web or as chapters in the edited volume *De staat van informatie* (The State of Information)), which provided the building blocks for this publication.

The research methods applied were highly empirical, and the results of the various underlying studies are described in separate publications. This book does not report

directly on these studies, but instead builds its arguments on the data they gathered and on the other sources. The empirical chapters in Part II should therefore not be seen as case studies. Rather, they build on the material gathered in the underlying studies and discuss at length the insights arising from those studies. The empirical studies carried out especially for this book can be broken down into (a) domain studies, which review trends and developments in a broader policy context, and (b) 'black boxes', which concentrate on a much more specific area or a particular application. The black-box studies explore the dynamic information and technology-driven interactions between the various parties involved in developing technological applications. Many of the most crucial choices and interactions are still hidden from public view and have been explored in only a few academic or other publications. Mapping out the networks made up of systems developers, policymakers, institutions and users of technological applications – for example the biometric passport, the Electronic Patient Dossier or the Reference Index for Juveniles at Risk – reveals more about the dynamic impact that such applications have on the relationship between government and the citizen. Because the black-box studies focused on charting empirical trends and developments, they are relatively 'theory-lite'. George and Bennet (2004: 74) would call these 'atheoretical case studies', i.e. case material offering sound, detailed descriptions that do not contribute to theory themselves but can be used as input for other meta-research or more theoretical research.

In selecting the domain studies and black boxes for this book, we have attempted to cover all of the various factors and vantage points relevant to this study. We first consider the various roles of the citizen: passenger, patient, motorist, resident of a particular community, etc. Government also appears in many different guises in the empirical studies: as an initiator of new applications, a partner in public-private partnerships, a legislator and a regulator. Then there are the many different levels of government (international, European, national, local) and the interests, preferences and mutual relationships that operate at these levels. The applications and technologies explored here all play a role in generating, sharing and enhancing information, but from various vantage points and with different aims. ICT is now part of government in every sector and at every level, and it affects many different parties, roles and policy contexts.

The preparations for this publication involved writing a number of essays on broader or more conceptual issues in the domain in question. The subjects included government accountability in the information age, assessing the risks involved in information technology, the right to be 'forgotten' in a digitized criminal law system, and system responsibility for the information society as a positive human rights obligation. Finally – in cooperation with the ECP-EPN Platform for the Information Society and Centerdata research institute (Tilburg University) – we asked 2357 panel members to complete a questionnaire half way through 2010. Completed questionnaires were received from 1485 respondents (63%). The panel

is a representative sample of the Dutch population. All the underlying studies and essays were incorporated into the edited volume *De staat van informatie* (Broeders, Cuijpers & Prins 2011), published simultaneously with the Dutch version of this book), or on the WRR's website. Box 1.2 gives a summary of these background studies.

Box 1.2 Overview of background studies

Background studies in the published volume (D. Broeders, C. Cuijpers & J.E.J. Prins (eds) (2011) *De staat van informatie*, WRR-verkenning 25, Amsterdam: Amsterdam University Press; available for download at www.wrr.nl/content.jsp?objectid=5657

The published volume with background studies for the report *iGovernment* (*iOverheid*) contained pieces in three broad categories.

Two studies served to elucidate key concepts of the analysis. From different angles they dealt especially with the notion that government (public authority) carries a final responsibility of sorts for the way that the information society takes shape. This responsibility cannot be taken too far, because it is both factually and normatively unwise to assign government an exceedingly dominant role; yet at the same time it cannot be denied altogether due to the duty to protect and safeguard certain fundamental rights, also in 'horizontal' relationships.

In addition, some studies tackled themes concerning ICT and government that have an overarching relevance across policy areas and sectors. These involved an essay on 'the right to be forgotten' in a digital age that seems bent on remembering, especially remembering personal facts and profiles, and an essay dealing with technological risks and the question which actors are best placed to assess and bear the consequences of these risks, bearing in mind that some risky activities are quite worthwhile. Also included was a quantitative study on the nature of citizens' complaints about public sector ICT, and the way in which organizations deal with such complaints (in terms of registration and learning processes). Finally, a study dealt with the development of the office of CIO (Chief Information Officer) across the board of Dutch national government.

Lastly, there were broad studies on selected policy domains. These concerned the sometimes opaque process of digitization of the EU's borders through an (expanding) number of databases, the emergence of ICT systems meant to enable preventive and proactive measures in the domain of child welfare, and finally the digitization of medical records and the shifts that it brings about in the roles of those concerned (patients, doctors, insurers etc.).

Background studies published on the web (www.wrr.nl)

Studies of a more detailed and descriptive nature were published on the web. These covered a wide variety of subjects, but usually did focus on a particular ICT-application. Applications covered

were: the Electronic Patient Dossier (EPD), the biometric passport, the "Safe Houses" at municipal level, and eCall. Somewhat broader enquiries were undertaken into the way that ICT affects the privacy of people travelling (road, rail), into the institutions (especially ICTU) responsible for commissioning government ICT in the Netherlands, and finally (by way of a panel) into the opinion of the average citizen concerning the sharing of personal information between specified public and private bodies.

This book is structured as follows. It is divided into three parts and consists of nine chapters and an afterword. Part I*, Introduction and context*, comprises this introductory chapter and Chapter 2, which discusses various theoretical principles and concepts that provide tools for analysing the empirical material. Part II*, Empirical analysis*, devotes five chapters to charting and analysing the digitization of government in the Netherlands. The analysis mainly considers trends and developments, and the roles and interactions of the most prominent parties in the domain of digital government. Chapter 3 focuses on the political world. Chapter 4 looks at the dynamic relationship between politicians and policymakers in central government and the public authorities that implement policy, both nationally and locally. Chapter 5 shifts the perspective to the international and European arenas. Chapter 6 discusses the relationship between the public authorities and commercial parties, including the major new forces of the information society and the businesses that develop and create applications for government. Chapter 7 begins by looking at a number of government and other institutions that supervise or control the development of iGovernment in some way or another, and that play a role as a countervailing power. It then considers the public's role as a digital countervailing force. Part III*, Analysis and recommendations*, takes stock of the empirical research. Chapter 8 advocates a paradigm shift in government's approach to digitization, arguing that the prevailing concept of eGovernment should be replaced by that of iGovernment. Chapter 9 describes the paradigm shift in terms of policy, procedural and institutional recommendations that should make 'iGovernment self-awareness' inherent not only in how government acts but also in how it is organised and how it thinks. The epilogue outlines government's broader responsibility in a rapidly changing iSociety.

NOTES

1 Which translates roughly into 'howmycouncilvotes.nl'.

2 In December 2009, the Obama Administration issued the *Open Government Directive* requiring federal agencies to take immediate, specific steps to support "open government", based on the principles of transparency, participation, and collaboration. These steps must ensure that federal agencies always publish government information (to the extent permitted by law and subject to valid privacy, confidentiality, security, or other restrictions) (www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-06.pdf).

3 The British Government has made thousands of datasets publicly available at www.data.gov.uk. Individual citizens, organisations and developers may search through the datasets but also copy and recycle information. The website also has a wiki for sharing information on techniques used to process the data.

4 "The Dutch Government wishes to be transparent about the legislative process and make greater use of the public's knowledge in preparing legislation. Starting on 24 June 2009, it will therefore begin informing citizens, companies and civil-society organisations about impending legislation online. It is also making it possible for citizens to offer suggestions and proposals for new legislation online. This is a nation-wide experiment that will run for two years" (translation of text on www.internetconsultatie.nl, consulted on 3 November 2010).

5 Compared with its predecessor 'Towards a safer society' (*Naar een veiliger samenleving)*, the fourth Balkenende Government's 'Safety begins with prevention' programme (*Veiligheid begint met voorkomen)* explicitly combines prevention, administrative and criminal law enforcement, and follow-up (Tweede Kamer 2007-2008b).

6 Interview with Mr Marcel van Asperdt, head of Expertise and Innovation, National Communications Security Agency (NBV), July 2010; interview with prof. Bart Jacobs, professor, Radboud University, June 2010.

2 ANALYTICAL FRAMEWORK: INFORMATION, ACTORS AND PRINCIPLES

Commentators have noted countless times that digitization is having an unprecedented impact on society. The dozens of reports published on ICT in recent years use adjectives such as *revolutionary* developments, *unique* opportunities, *complex* tensions, *fundamental* changes, *shifting* interests and *obsolete* social and institutional contexts. But why, precisely, is digitization having such an unparalleled impact? Why should commentators refer to the related opportunities, tensions, shifts and challenges as 'fundamental', 'unique' or 'complex'? And if all that is true, what are the consequences of digitization for the relationship between government and the citizen? If we set these qualifications to the side and examine the features that make ICT 'different' or 'new', we see that the nature of digitization is less uniform than it may at first appear. Although the term 'digitization' suggests a clear-cut, well-defined phenomenon, everyday reality teaches us that it in fact consists of a wide variety of trends and developments, technological breakthroughs and specific applications. Each of these trends, breakthroughs and applications is initiated and, gradually, influenced by the many different actors involved, their interactions, and the foreseen and unforeseen consequences of those interactions. The next chapters (in Part II) attempt to make sense of the dynamics between actors, processes and interests, with the analysis focusing specifically on the relationship between government and citizens (individually or collectively). Our description of empirical reality in the Netherlands will help us understand the impact of digitization on that relationship. Before we begin our empirical analysis, however, this chapter offers an analytical framework. It also discusses the main issues and key concepts explored in the rest of the book.

As stated previously, the analysis presented in this book focuses less on individual technologies than on the role these technologies play in the relationship between different actors. In other words, it studies the 'sociotechnological complex', and explores the interplay between technology and information from that perspective (Section 2.2). The chapter goes on to offer a descriptive and normative framework for charting empirical reality. The emphasis is on practical developments and actual shifts in the various actors' positions, authority and influence. Section 2.3 defines the main actors: government, citizens and technological applications. Section 2.4 then introduces a normative framework for describing the dynamics of empirical reality. It divides the many different, widely varying principles (e.g. efficiency, transparency, and freedom of choice) that turn up again and again in policy proposals and public and political debate into three clusters – driving principles, underpinning principles, and process-based principles. The dynamics between these three clusters give us an important normative and analytical tool for identifying and explaining the empirical developments discussed in Part II.

2.1 VIEWS ON THE RELATIONSHIP BETWEEN TECHNOLOGY AND ITS USERS

This book examines the impact of using ICT on the relationship between government and the citizen. Anyone embarking on such an examination must first clarify precisely how the role and influence of technology are interpreted. Is technology – whether we mean a public transport chip card, biometrics, or a security camera – nothing more than a neutral tool wielded by citizens, politicians and policymakers? Or is it in fact an irresistible force that follows its own logic and, in doing so, also has its own separate impact? These questions touch on an academic debate about the conceptual interpretation of technology and the factors that can be emphasised when studying technology, society, and the interaction between them. Opinions expressed in the literature are by no means unanimous in this regard. Although our analysis does not do full justice to the wide-ranging academic debate about the nature and role of technology in society, we can basically divide the views put forward in public debate and in political and administrative reality into three approaches. At one end of the spectrum is instrumentalism, and at the other there is technological determinism. The middle ground between these two extremes consists of a dense multidisciplinary field that is more constructivist in its approach. Because this study focuses on the relevant actors – the citizen, government, and the 'application' – and examines the interaction between social and technological influences, it can immediately be identified as constructivist. Before examining this middle ground in more detail, we will look more generally at the broader spectrum of viewpoints. After all, all three approaches are applied, more or less explicitly, in public debate.

2.1.1 FROM INSTRUMENTALISM TO TECHNOLOGICAL DETERMINISM

According to the principles of *instrumentalism*, technology is a neutral and valuable tool that can be used in many different ways. Technological applications are the neutral bearers of their designers' ideas and aims. Social change takes place autonomously and drives technology forward. In this view, technology offers an excellent solution to all kinds of problems; it is a multifunctional instrument (Kaplan 2009: xvi). As a result, politicians are quick to turn to technology to solve problems, including societal ones (see also Van den Berg et al. 2008). That is not to say that instrumentalists are convinced that technology will lead to good results every time. If the outcome is disappointing, it is the users who are to blame, and not the technology (Van de Donk & Depla 1993). That is because technology is regarded as value-free, a mere 'instrument' in the hands of those who can use it either for good or evil. Although the notion of technology as a neutral instrument has lost popularity in academic circles in recent decades, it is often still very much alive in government, according to recent reports by the Netherlands Court of Audit (Netherlands Court of Audit 2007; Edge 1995; MacKenzie 1999a: 43).

Box 2.1 Citizen Service Number (BSN): neutral instrument or force that follows its own logic?

During the Dutch Parliament's discussion of the bill introducing the Citizen Service Number (BSN), the Minister responsible stressed that this unique personal number was nothing more than an information number, suggesting that its consequences and impact would be neutral. The Confederation of Netherlands Industry and Employers (VNO-NCW) agreed with this view unequivocally, stating: "Our overall comment is that the BSN does not pose a risk in itself. It is a neutral number. Any data-sharing that is prohibited without the BSN will also be prohibited with the BSN" (Position of VNO-NCW in BSN discussion with the Data Protection Authority, 30 January 2006). However, various parliamentary parties in both the House of Representatives and the Senate noted that the BSN facilitated the 'increasing informational power of government' (Tweede Kamer 2005-2006c: 1). Concern was also expressed that the BSN would lead to both public and private-sector organisations changing their working methods and information requirements (Eerste Kamer 2007-2008). Since then, various cases have shown that the BSN is clearly more than just a neutral tool; it is developing into an appealing policy vehicle. Some examples: a bill is now being prepared to allow the BSN to be used in the financial sector (Eerste Kamer 2009-2010f); there was a heated discussion in mid-2010 between the Data Protection Authority, the Ministry of Infrastructure and the Environment about displaying the BSN on the Civil Service Smartcard (*Rijkspas*) (CBP 2010a); and the Ministry of Economic Affairs is investigating whether the BSN can be used for electronic authentication ('eRecognition') by companies and self-employed people who make use of digital service delivery (Leenes, Koops & Van der Wees 2010). The State Secretary at the Ministry of the Interior and Kingdom Relations stated in late August 2010 that she did not see any reason to draft an overarching evaluation framework for the use (or wider use) of the BSN (Eerste Kamer 2009-2010f). At that point, more than two years had passed since Parliament had asked the Government to indicate a feasible evaluation framework (Eerste Kamer 2007-2008).

Technological determinism is based on the assumption that technology plays a crucial role in shaping society. Technology is depicted as an irresistible force that follows its own logic and has a major impact on the way work, the economy, and society as a whole are organised (Williams & Edge 1996: 55). As far back as 1996, Frissen concluded that the instrumentalist view of technology so prevalent in the modern pursuit of control had become almost untenable considering its autonomous power (Frissen 1996: 344). More recently, Socialist Party MP Ronald van Raak made the following comment at general parliamentary consultations on the national database of biometric features.

"The tools will determine the morality. Imagine that such a database exists. A terrible crime is committed. The police naturally want to solve it. And if the option is available to them … Create the database and you create a use for it. It is obvious that the database will be used for all kinds of other purposes in future. I'm sure the State Secretary is well aware of that" (Tweede Kamer 2010-2011a: 15).

There are various gradations of technological determinism. In the most extreme case, technology is reason enough for behaviour to change, and even for whole societies to be transformed (Chandler 1996). In the milder variety, technology is still the most decisive factor, but not the only one (MacKenzie 1999b). Technological determinism, furthermore, can take both an optimistic and a pessimistic view of technology. The optimists believe that everything technologically possible will come to pass and will benefit society (Van den Berg 2009: 42). The pessimists agree that everything technologically possible will come to pass, but they believe that society will be 'overwhelmed' and 'suffer a loss of autonomy and solidarity'. They fear a world driven by technological rationalism, with little regard for the human dimension (Ellul 1954; Ellul 1977; Anders 1980).

As noted above, this book takes up a position in the middle ground between instrumentalism and technological determinism. A wide-ranging group of researchers can be found in this middle ground; although they represent different intellectual traditions, they agree on the need to open 'the black box of technology' (MacKenzie & Wajcman 1985; Bijker & Law 1992; Williams & Edge 1996: 54). Partly as a reaction to technological determinism and instrumentalism, a new, interactive view of technology emerged in the 1980s and 1990s, based on the assumption that technology and society influence each other (Fuglsang 2001). Proponents of this idea study technology and technological concepts in relation to social reality, and not as a separate domain (Kaplan 2009), and regard technology as both a cause and an effect of societal change (Williams & Edge 1996: 55). This *constructivist* view focuses in particular on the development process of specific technological applications and the role that the relevant actors play in that process. The main idea is that the form that a technological application ultimately takes is the result of various choices. A technological artefact does not simply appear out of nowhere; it is the outcome of existing social, economic and technological relationships (Bijker & Law 1992). In addition to the social constructivist view of technology, the focus has also shifted to the workings of technology itself. Once a technology has come to play an established role in society, it is difficult to change it. People have invested in a certain configuration and use the application in a certain way, making it part of a network of practices and institutions. In that sense, technology 'determines' social evolution (Bijker 2001: 28-29), but that does not mean that 'mature' sociotechnological systems are entirely inflexible; it simply implies that it takes much more effort to change them.

2.1.2 THE SOCIOTECHNOLOGICAL COMPLEX AS A SUBJECT OF RESEARCH

This study is based on the idea that social relationships mould technology and that technology simultaneously influences social relationships. It takes this idea as its point of departure because the aim is to examine the consequences of using ICT for the relationship between government and the citizen, examining ICT as part of a dynamic convergence of multiple processes, interests and actors. In keeping with the constructivist view, we will refer to this complex network of institutions and technological applications as the sociotechnological system. Part II of this book looks more closely at the impact of using ICT on the relationship between government and citizens by reviewing the sociotechnological systems associated with applications such as the Reference Index for Juveniles at Risk, the biometric passport, eCall, and the national Electronic Patient Dossier. The empirical analysis in Part II focuses on three points.

The first of these is the role of the *actors*. The way in which technological applications are developed and used clearly depends on the interests, ability to influence, views, knowledge and skills, expectations, values, and perceptions of the relevant actors (developers, policymakers, users and non-users), as well as on the technical possibilities and impossibilities (Stirling 2008). This also includes the balance of power. Which actors are capable of controlling the development of a technology, and which are not? The occasional battle over the way an application should be designed and used is not fought on a level playing field. Indeed, there are different levels of influence and power at play in the interactions between institutions, cultures and systems (Mansell & Silverstone 1996: 213). For example, the end users of a technology may not have a say in its development, and the behaviour of actors that have no direct stake in the technology may still be affected by it. Chapter 3 points out the gap between the policymakers who order an application to be developed and implemented and the professionals in the field who actually end up working with it but have had no say in its development.

The second point in the analysis is *time*. Hughes (1994), for example, emphasises that organisations, groups and individuals exert a huge influence in the development phase of a technology. As time passes, however, and as an application becomes embedded in society, the system's complexity increases and the technology becomes harder to control; it acquires its own momentum. Once a technology has been developed and delivers certain services, and once time and money have been spent on it, it becomes difficult to make fundamental changes (Hughes 1994). In fact, technology develops in three stages. In the first, there is a great deal of 'interpretive flexibility', the application is still 'open', and various interpretations and choices are still possible. Designers, clients, the authorities, consultants, researchers and the intended users all have their own ideas about how the technological application ought to work. Pinch and Bijker (1984: 414) refer to 'relevant

social groups' that influence the development process, either in an organised way or ad hoc. Keymolen & Prins (2011), for example, show in their study of the Reference Index for Juveniles at Risk (VIR) that early on, system developers and consultants at the local level had a fair amount of influence on the system's information design. In the next stage, when the application assumes its final form, it is at least in part a reflection of the relationships, convictions and interests of the actors involved in its design and implementation (Woolgar 1996: 87-88). In the final stage, the application moves into a broader social and political context and may in its turn influence social relationships. Or, as Johnson and Wetmore put it (2009: xiii):

> "Once created, sociotechnical systems can sometimes seem to take on a power of their own. They facilitate and constrain certain actions and thereby facilitate and constrain certain values. In other words, the intertwining of society and technology is not neutral; it is value laden."

The final point is the *level of analysis*. In the first instance, we look at how a specific technology develops and who is involved in its development. In addition, Part II also takes macro-level trends – for example economic interests, international law, globalization and the demand for security – into account, not in the least because these trends and developments influence the actors, their interests, and the context in which a technology takes shape. Mapping out both the processes involved in a specific technology and the wider social changes affecting these processes produces a multi-layered picture of the role ICT plays in the relationship between government and the citizen.

2.2 TECHNOLOGY AND INFORMATION

Of the dual concepts technology and information, this study focuses primarily on the latter, and more specifically on the way in which various actors influence and change how information is used. The 'informational' side of ICT cannot be viewed separately from technology, of course. For example, the use of biometrics in passports has shown that technology determines the sort of information that is or can be collected. Technology also facilitates certain information flows or dictates who has access to information. It is the software that allows an Electronic Patient Dossier (EPD) managed by an individual care provider to be accessed by other care providers. But we can only study precisely how a certain technology allows information to be gathered, used and shared by looking at specific applications and connections. In this book, then, the emphasis is not on biometrics or network technology (the technology), but on the biometric passport and the digital dossier (the application). ICT then stands for all technological applications used to gather, store, process, enhance and share information.

2.2.1 FROM DATA TO INFORMATION TO KNOWLEDGE

A close examination of the 'information' component of our pair of concepts reveals that it comes in many different guises, depending on what stage of processing it is in. First, data is gathered and recorded electronically. Data as such is meaningless. It has not yet been filtered, interpreted or processed. It does, however, represent a fact. A distinction is sometimes made between 'raw data' and 'data' – in other words, data that has not been arranged in any way versus data that has been arranged to some extent. This report uses the two terms synonymously. Data becomes information when we select only the data relevant within a certain context and for a certain group of users. In other words, information emerges when we arrange and link up data within a system and for a particular purpose, policy-related or otherwise. Or, as Liebenhau and Backhouse (1990) put it: "Information is data arranged in a meaningful way for some perceived purpose" (in Canhoto & Backhouse 2008: 48). It is therefore not evident that gathering more data automatically produces more information. Indeed, an excess of data can result in 'noise', making it difficult to distil information from it. Finally, interlinking and applying various information components gives rise to knowledge. Knowledge mainly becomes valuable when it is used for and gives rise to action (Van der Lubbe 2002).

Society today is often depicted as an information society (Castells 1996) or knowledge society (WRR 2002). Traditionally, property, labour and money were the most important means of production; in recent decades, however, information and knowledge have become the new 'capital'. ICT now makes it possible to collect, store, process and share data on an unprecedented scale (Mayer-Schönberger 2009). It is important, however, to remember that information has always had economic and social value. No society can survive without ensuring, in one way or another, that information – and knowledge – are shared and passed on (Porter 1995: 45). Whether in the form of oral tradition, symbols, printing, film or ICT, mankind has filtered, retained and handed down information throughout history. Information gathering has always been a key factor in statehood, for example. It also had an emancipatory function. By giving every *citoyen* an identity, Napoleon allowed the masses to free themselves from aristocratic hegemony. It was, however, the rise of the bureaucratic state that also led, inevitably, to the collection, classification and storage of information on citizens. Scott (1998) observes that a state attempts to make society 'legible' by gathering information. Individual citizens are registered as taxpayers, conscripts, employees and so on (see also Caplan & Torpey 2001: 1). That information and 'legibility' are crucial to the state's power to govern society. Authors such as Weber and Foucault regarded bureaucracy as a highly rational system of information gathering and administrative control. Torpey (1998) also pointed out that the state's ability to 'penetrate' social processes depends on its capacity to 'embrace' society: "As states grow

larger and more administratively adept they can only penetrate society effectively if they embrace society first. Individuals who remain beyond the embrace of the state necessarily represent a limit on its penetration" (Torpey 1998: 244). The tendency of governments to gather as much data as possible – Sheptycki (2007) refers to their 'compulsive data demand' – is strong and does not appear to be weakening in today's information society.

2.2.2 IT'S ALL ABOUT ACCESS, CONTROL AND KNOWLEDGE

The importance of information as such is not, however, what makes our current information and knowledge society what it is. Rather, the interplay between technology and information has two notable features, which are highlighted in this study: (1) the way in which information is or is not made accessible, and (2) the way in which information is selected and converted into knowledge.

To begin with, it appears that the extent to which and the way in which information is or is not made *accessible* is becoming a defining factor. Indeed, ICT is a powerful tool both because it provides access to new or existing information and because it can manage and control such access (Dutton 1999: 11-12). The importance of access and, consequently, of information-sharing becomes clear in the case of the Reference Index for Juveniles at Risk (VIR). The primary aim of this project, which is intended to prevent the tragedies of child abuse and neglect, is to improve information-sharing between youth care organisations, in particular those that do not usually communicate with one another. Whereas information used to be shared only among friends and acquaintances, ICT now also makes it possible for people who do not know each other to communicate and interact – and in fact it is used particularly for such communication (Porter 1995: 46). Important factors in this regard are (1) linked data, (2) the ability to quickly and easily copy data, and (3) the persistence of data (Van den Berg & Leenes 2010).

Individuals and organisations are disclosing and sharing more and more information about themselves and others, and the digitization of that information makes it much easier to disseminate and interlink it in both the public and private domains. Information also migrates easily from one context to another, blurring the distinction between the public and private realms. For example, information generated by the public transport chip card can be accessed by several dozens of parties in both the public and private sectors.

One vital issue related to accessibility is control. Who controls access to information? Control and access cannot be considered separately from the technological application or the medium that carries the information. For example, the Internet makes it possible to disseminate and share information with an infinite number of people without this being subject to much centralised control. This differs from

the databases and systems of the Netherlands' Tax and Customs Administration or General Intelligence and Security Service, to which access is strictly controlled. Fleck (1993) distinguishes between technologies set up as 'systems' and those that constitute 'configurations'. A system is a restricted network in which coordination between the components is strictly defined, making centralised monitoring and control possible. Systems retain their form and meaning in varying contexts. A configuration, on the other hand, is an open network consisting of various branches and applications, making centralised monitoring and control more problematic. Users play a much larger role in defining how a configuration functions than they do in a system. No single actor can be said to manage information flows in society. Some argue that mass access to PCs and the Internet is giving users more control over their own information (Gilder 1994; Dutton 1999; Frissen 2008; Leadbeater 2007); others claim that ICT advances are creating a new elite of 'cybercrats' or 'numerati' (Ronfeldt 1992; Baker 2008). And experience teaches us that information is not always available, or available to everyone – as illustrated by a government initiative to 'blacklist' certain Web pages in cooperation with Internet service providers. The blacklisted pages are blocked and therefore cannot be accessed by the public.[1]

But there is more at stake than access to information and access control. The greatest challenge today is not to collect more data – that happens 'automatically', as it were – but to use the masses of data to glean *relevant* information and, ultimately, *knowledge* with a particular purpose aim in mind (Hildebrandt & Gutwirth 2008: 1). In addition to access and control, the second significant feature of the information and knowledge society is the way in which *information is converted into knowledge.* That challenge applies equally to deciding *which data will or will not be converted into information.* In short, the issue is not information as such or how much of it we have, but its relevance and our ability to distil knowledge from it. In order to cope with the overwhelming amount of data available, we continue to optimise our information selection processes, and that often involves digitization. The best-known example of this is the search engine Google, which uses an algorithm to classify websites according to the user's search terms and then quickly opens a link to the Web page with the 'right' answer. The use of algorithms to search for notable patterns or correlations in data is known as data mining (Custers 2004). Data mining produces correlations that indicate a relationship between different data without necessarily divulging the causality of that relationship (Hildebrandt 2008: 18). Another well-known data-mining application is the service offered by the online bookstore Amazon.com: "Customers Who Bought This Item Also Bought . . ." Data mining leads to profiles (a collection of correlated data) – a process known as profiling (see Canhoto & Backhouse 2008). Information on consumers' online purchases, the behaviour of young people, or the spending patterns of benefits recipients can be categorised and used statistically to predict their future behaviour. Profiling also takes place along two axes: the individual's past behaviour (purchasing history, pattern of illness, etc.) and past mass behav-

iour. The correlations represent the likelihood that past patterns will repeat themselves in the future (Hildebrandt 2008: 18; Raab 2009). Profiles are not only used in the commercial sector; government also uses profiling in various policy areas (taxes, social insurance, youth healthcare, surveillance and enforcement). 'Citizen profiles' make it possible for government to take a more individual approach, to focus on target groups, and to reduce the administrative burden imposed on citizens or eliminate the need to 'bother' them (Van der Hof et al. 2009).

Box 2.2 Risk profiles

One example of a fully automated risk analysis based on risk profiles can be found in the new approach to monitoring legal entities (Tweede Kamer 2008-2009f). The current system of preventive monitoring is to be replaced by permanently automated monitoring based on risk analyses. The new system will also make use of data on individuals, for example the children and grandchildren of company directors. The risk analysis is based on risk profiles and risk indicators established at regular intervals by the Ministry of Justice. Each risk profile consists of a set of risk indicators (indicating the risk of abuse) or characteristics that, when taken together, may indicate a form of abuse. The involvement of family members (children and grandchildren) in the legal entity is an example of a risk indicator. The data included in the analysis is taken from the Tax and Customs Administration, the Land Registry, the Trade Register, the Municipal Personal Records Database, police files, and the records of organisations responsible for implementing employees' insurance schemes. The greater the number of risk indicators that are flagged in a particular case, the higher the legal entity's risk score. Every change in the legal entity's 'life course' is subject to automatic analysis based on the risk profiles. According to the explanatory notes to the bill, such 'life course changes' run to several hundred thousand a year. Monitoring of a legal entity may be stepped up depending on its risk score. The risk reports are distributed entirely automatically to various enforcement officials designated as such by an Order in Council. It is not necessary to inform individuals that their data is being used in a risk report.

The Government's wish to be proactive is boosting the popularity of profiling in the public sector, but it sometimes goes further than merely identifying and categorising people. It aims to use the knowledge thus generated to anticipate future developments. Profiling technologies not only help predict the obligations, rights and requirements of specific individuals at the earliest possible stage, but also help to manage, guide and regulate them in good time. For example, the police now work with Prokid, a tool for tracking under-twelves who have been connected in some way or another with a criminal offence (including those who have only witnessed a crime). Prokid assesses risk based on two sources of information. First of all, it uses behavioural indicators thought or known to lead to criminal activity. Secondly, it considers data on other people in the under-twelve's household and assesses whether they indicate a higher risk of criminal or problem behaviour in the juvenile. Based on these two data sources (the child and his or her living envi-

ronment), Prokid then assigns the child to a risk category. The tool makes early detection of the risk of criminal or problem behaviour in children possible (Keymolen & Prins 2011).

Box 2.3 False positive and false negative risks at the airport

There are two types of error that can arise when using risk profiles or new technologies such as biometrics; each with very different repercussions. A case in point is the biometric passports recently introduced in the Netherlands. At passport control, an airline passenger's fingerprint will be compared with the fingerprint stored in the passport to determine whether they match.

Besides correct findings (e.g. the passenger's fingerprint is the same as the fingerprint in the passport), the comparison can also produce a *false negative outcome* (the passenger's fingerprint does not match the fingerprint in the passport, although it is in fact the same person) or a *false positive outcome* (the passenger's fingerprint matches the fingerprint in the passport, although it is *not* the same person). The first error leads to frustration for the traveller, extra checks into his or her identity, and – in many cases – a missed flight. The second allows people to enter the country who should never have been admitted. The ultimate fear is that irregular migrants, criminals, or even terrorists will be allowed in.

The technology used at airports, however (such as biometric access systems), allows the officials responsible to simply 'set' the margin of error, and that is precisely what they do. Fingerprint recognition can, for example, be set at 99 per cent certainty, or at 80 per cent. The first means stricter surveillance and long lines at passport control, but it reduces the risk of a false negative outcome (admitting people who do not match their biometric passport) to almost zero. The second keeps lines moving at the airport but increases that risk. The security services will usually argue in favour of the first option, whereas commercial and economic interests – including the state – favour the second. Trade-offs between the two are possible. In that sense, false positive and false negative errors are communicating vessels to some extent.

Growing awareness that the challenge is not simply to gather large quantities of information but to trace *relevant* information and generate new knowledge has led to another item being placed on the agenda: information about information, i.e. metadata. Because technology makes it possible to collect and interlink more and more data, there is a rising demand for technology to help trace data, make it permanently accessible, and structure it. Metadata (data that says something about a specific set of documents or a chunk of information) plays a key role both in making data permanently accessible and in structuring it. Many of today's technological applications are designed to automatically generate data about their activities or products. A fax machine automatically adds the date to incoming and outgoing faxes; a digital camera 'remembers' when a photograph was snapped; a camera with GPS records where a photograph or film was made; and some cars

'remember' their speed at a particular time. Such data on the relevant item (fax, photograph, film or car) makes it easier to organise and retrieve information. Metadata is also playing an increasingly important role in the relationship between government and the citizen in that it influences the power relationships of the actors involved.

One significant development when it comes to searching for and finding relevant information is that indexes and search functions are now being integrated into a single interface, allowing all the various information levels to be displayed at once. In other words, the old-fashioned distinction between searching in folders (card files) and searching in files (the actual content) is becoming blurred (Mayer-Schönberger 2009:77). At the same time, new tools are making it possible to use metadata to regulate access. For example, it is now possible to use the metadata for a file (a book, article, film, piece of music, etc.) to define who has access to the relevant information and to what extent (read-only or editable). There have now been calls to regulate the ownership and use of metadata, based on the growing awareness that "metadata, concentrating the sea of data to make it comprehensible, also can act as a bottleneck on information access and is an instrument of market power" (Cukier 2010:10).

2.3 FOCUS ON THE ACTORS

The previous two sections outline the overall approach of this study. Basing the analysis on the sociotechnological system means that it will focus on the interplay between the various actors involved. It is this interplay that ultimately shapes the dynamics between information and technology. The actors were identified by means of empirical research into specific applications and a study of the literature, which took the form of domain studies focusing on the broader policy area. The empirical research, the literature study, and interviews conducted with professionals working in the field of 'ICT and government' constitute the building blocks for the strategic agenda set out in this book. The aim is to identify general patterns and insights by analysing various applications. The most prominent actors considered here are the citizen, government and the application. They are naturally not the only categories that influence the development, implementation and impact of ICT. Business, industry and interest groups often play an important role as well, but this study considers them only when they affect the interactions between the three main actors, which are introduced in more detail below.

2.3.1 THE ACTORS

The labels 'citizen' and 'government' are useful abstractions. They are constructs that allow us to consider how actual citizens or actual public authorities relate to one another and to others. In fact, the 'citizen' consists of many different citizens

and 'government' of many different public authorities whose interests and preferences may in fact conflict – although 'government' (i.e. the state) does function as a single entity in its legal and political relationship with citizens. A different level of abstraction is needed to regard 'applications' as an actor, as one cannot ascribe free will to an application. Technology can, however, influence human behaviour through the design and function of an application.

2.3.2 'APPLICATIONS'

Technology, and more specifically the technological application, is the odd man out in our trio of actors. The term 'actor' is associated with 'action', and action is often taken with a certain conviction or intention. The fact that applications are regarded as actors in this analysis does not mean that intention or autonomy have been ascribed to them. The main reason for regarding an application as an actor is that its presence 'does something' in interactions. An actor is something or someone who makes a *difference* in a relationship (Latour 2005). In other words, technological applications such as the EPD and the biometric passport to an extent shape the relationship between citizens and government. Their presence or absence makes a difference. In order to understand why actions take place and how citizens and public authorities interact, our analysis should also consider the items that make these actions possible. We have already noted that technological applications influence the behaviour of citizens and public authorities. Applications that are embedded in society tend to take on a life of their own, making change difficult and impeding or stimulating certain human behaviour. Technological applications also have both intended and unintended consequences that influence the interaction between actors and their modus operandi. For example, when mobile phones first appeared in the market, text messaging was nothing more than an amusing extra feature. It unexpectedly became so popular that it has not only become a significant communication channel (certainly for young people), but has also had an impact in all kinds of other areas, for example the evolution of language.

It is clear from the way people deal with computers, televisions, telephones and other technology that applications also possess agency – the capacity to act – in everyday life. Psychologists have found that people apply the same rules in their interactions with computers and TVs that they apply in interpersonal interactions (Reeves & Nass 1996). This is sometimes referred to as the CASA paradigm, for Computers Are Social Actors (Nass et al. 1994; Nass et al. 1995). It is, once again, not necessary to ascribe intention or autonomy to computers. Computers do not have emotions, but they can evoke an emotional response in their users, leading them in turn to believe that their interactions with technological applications involve an emotional investment (Nusselder 2007: 9). The fact that people treat computers like social actors encourages designers to add features such as speech technology and feedback information to some applications in an attempt to live up

to these expectations (Klein 2003). They also deliberately design expert systems to take over the user's capacity to act. Examples are the automatic pilot function in aircraft, which takes over various controls from the human pilot, and the automatic car brake system, activated when the car ahead abruptly reduces speed. ICT can also structure and even control the relationship between government and citizens. Bovens and Zouridis (2002) have noted that the 'street-level bureaucrat' is becoming a 'screen-level bureaucrat'. Professionals are witnessing the decline of their discretionary power owing to the menus and decision matrices programmed into the software they use (see also Meijer 2009; Lyon 2009). It is the application that now decides what information is relevant and correct, and it is the managers or bureaucratic officials who decide what application is to be used. In this 'infocracy' (Zuurmond 1994), what professionals do – and what they perceive – increasingly depends on the applications they work with. Some local reference indexes for juveniles at risk are designed to "include young people 'automatically' if the intake flags them as requiring assistance based on certain criteria" (Holla et al. 2008: 13). In short, it is no longer the doctor, youth social worker or other professional who decides whether the system is marking a child as at risk.

It is also not always possible for users to check the accuracy of an application's output. The computer produces ready-made figures, statistics and alerts, and the user simply has to trust the information it delivers. Van den Hoven (1998) describes these applications as 'artificial authorities'. Users depend, for the most part unilaterally, on the information that they produce. Neither users nor professionals are mere hapless victims of ICT, however. They seek out workable solutions within or outside the system, thereby guaranteeing that humans remain in control (Van den Akker & Kuiper 2008).

2.3.3 'CITIZENS'

It should come as no surprise that the definition of 'citizen' can be broken down into many different individuals or groups of individuals. Within the context of this book and its subject, this breakdown takes place along two axes: the relationship between citizens and information technology and the relationship between government and citizens.

People differ considerably from one another when it comes to their relationship with information technology. They have different levels of knowledge, different skills, different attitudes, and different needs and requirements. Although ICT has become an indispensable part of everyday life, Dutch people have taken it on board at different speeds, and not everyone has plunged into digital life with the same abandon. Alongside those who have embraced ICT with enthusiasm, there are others who deliberately refuse to join in (Wyatt 2003; Van Dijk 2007; Van den Berg 2009) or who cannot keep up with the lightning-fast changes, especially the

elderly, people with limited education, low-income groups, and some ethnic minorities (CBS 2009a; Van Dijk 2007). It is often impossible to predict what will and will not prove popular – a process known as the 'domestication of technology' (Frissen 2004). That process – described by Silverstone and Hirsch (1992) as "a taming of the wild and a cultivation of the tame" (quoted in Oudshoorn & Pinch 2003: 14) – changes both the user and the technology. ICT can also have a major impact on the roles that citizens play and may fulfil various needs and requirements. The political activist, the patient suffering a rare illness, the expat who wants to stay in touch with family back home, or someone who simply wants to be part of a social network are all living increasingly digital lives.

The public authorities and citizens are also increasingly interacting in digital environments, the latter in the role of client, taxpayer, patient, campaigner for public order and safety, and voter. The positions and interests involved in these roles may conflict: a patient wants good healthcare and in that role probably supports the EPD, but the same patient may have also joined a support group website that lobbies for policy reform. As a politically engaged citizen, he or she may also be quite concerned about the privacy issues related to the EPD. Different people may have conflicting interests, certainly when it comes to the meta-role that technology plays in everyday life and government policy. Some are not worried about the information that the authorities gather about them, whereas others are fanatical in their support or opposition. Still others simply do not give it a second thought. Recent research shows that public opinion is becoming increasingly divided about the use of information. Respondents to the survey carried out by WRR, ECP-EPN and Centerdata have very specific ideas about who should be permitted to use what digital data and for what purpose (Attema & De Nood 2010: 2). They also want something in return for supporting such initiatives: more opportunity to inspect and correct data. For example, more than 80 per cent believe that professionals in the youth social work and healthcare sectors should be allowed to review digital data, but 70 per cent also think that parents or patients should be able to consult and review such data, and be told who else has access to or received the information (Attema & De Nood 2010: 2).

In terms of the information itself, the information society gives people both more and less leeway to present themselves in different guises. Sites devoted to social networking (Facebook) and professional networking (LinkedIn) enable members to present themselves to the world – or, in any event, to a smaller digital circle of acquaintances – as they wish to be seen. At the same time, the individual who puts that information on the Internet rapidly loses control of it (Mayer-Schönberger 2009). Information can turn up in contexts entirely different from what was intended, with everything that implies, and because the Internet is a network, that information is disseminated rapidly. How an individual is perceived and what information becomes available about him or her therefore depends only partly on

that person's own behaviour. Both businesses and the public authorities take a profound interest in the public in its many guises, both individually and collectively (Baker 2008; Mayer-Schönberger 2009). Mayer-Schönberger (2009: 104) reports that there are US providers of marketing information that offer more than a thousand individual data points for each of the millions of Americans in their databases. Increasingly, public authorities and businesses are approaching 'citizens' and 'clients' on the basis of their digital personas, as stored in various databases (Baker 2008). Special software makes it possible to search for patterns in the masses of stored data, allowing for profiling and data mining, the two best-known examples. According to Clarke (1988), surveillance is therefore increasingly turning into 'dataveillance': businesses and the authorities no longer monitor people by observing them directly, but by collecting and analysing existing information on them and their behaviour. Haggerty and Ericson (2000: 613) refers to 'data-doubles', or electronic profiles – often compiled from a combination of data fragments about a particular person – which are eventually used independently and come to lead a life of their own. Clarke (1994) refers to the 'digital persona' and Solove (2004) to 'digital persons'. This particular data strategy has significant implications for people: their digital identity increasingly consists of decontextualized information that is virtually impossible to erase from the digital memory of 'the Net' and the data gatherers who make use of it (Mayer-Schönberger 2009; Prins 2009; Buruma 2011).

Box 2.4 Citizens do not object to being 'traceable' on the Internet

The police do more than just walk the beat; they also patrol the Internet. They investigate social networking sites like Facebook for clues that they can use in their investigations. The tax authorities also search the Internet for relevant data on taxpayers. Dutch citizens who took part in the ECP-EPN/WRR survey gave both the police and the Tax and Customs Administration a lot of leeway to use 'public' data on the Internet (i.e. data that can be accessed without a password or some other security code). Eighty per cent of the respondents felt that the police should be able to trace data on the Internet. Almost 60 per cent believed that Tax and Customs should be allowed to search for public data on the Internet. Fifty per cent thought that the police should also be given access to secure or restricted data for investigation purposes. Almost 40 per cent said that Tax and Customs should be permitted access to Internet data that is restricted or secured (Attema & De Nood 2010).

2.3.4 'GOVERNMENT'

Government can also be broken down into many different subdivisions. Although 'government' is basically a single entity (nicely summarised in the Dutch Constitution, which defines the Netherlands as a decentralised unitary state), in everyday life it plays many different roles. It is active in different areas (politics, policy,

management and implementation) and operates through many different organisations (Tax and Customs, the police, and so on). It also breaks down into different entities in its relationship with the citizen. That is not really surprising: anyone who has dealings with the police sees a different side of government than in their transactions with Tax and Customs or their local council. And yet all of these represent the 'government' side of the government-citizen relationship and help define the political meaning of 'citizenship'. Like the citizen, government can be defined along two axes: the relationship between government and ICT, and the relationship between government and citizens.

ICT is also changing government, or rather, the various public authorities. Government information, communication and service delivery are rapidly being digitized, changing not only the public face of government but also many of its internal processes. In the same way that the 'ICT revolution' has affected the public, it has also influenced and continues to influence the public authorities in different ways and at different speeds. It has caused dramatic changes in information management and work processes (Dunleavy et al. 2006), but it is doing more than merely speeding up and streamlining Weberian bureaucracy. It is also transforming the way the authorities interact with other actors, both within and outside government. The interaction between government and citizens changes when a desk or an office becomes an Internet page, or when a passport becomes a fingerprint scan. What starts out as an updated version of the same – the way the first cars resembled carriages, but with engines – eventually takes on a life of its own. Recent decades have already seen the nature of government evolve in a direction compatible with the possibilities of ICT. Institutional differentiation, Europeanization, internationalization, and the liberalisation and privatisation operations of the 1990s have turned the Netherlands into a 'regulatory state', say Dijstelbloem and Holtslag (2010: 15), in a reference to Majone: alongside the traditional decentralised layers, 'government' has spread itself out across a multiplicity of government and quasi-government institutions. It has therefore increasingly turned into a network government, a development that is consistent with and closely tied in to the network potential of ICT.

The way in which government uses ICT and digital networks depend largely on the nature of the relationship between the citizen and government. From the vantage point of government, that relationship can be broken down into three categories of tasks: service, care and control. These are naturally very broad categories[2] that can be differentiated analytically, but tend to overlap considerably in reality. There are various reasons for this. eGovernment (as out-lined in Chapter 1) initially evolved from the drive to improve government service delivery and make it more efficient. More recently, however, ICT has also become popular in the general care sector (e.g. welfare, healthcare or youth care) and in the control and enforcement sector (e.g. the police, immigration and counter-terrorism).

Box 2.5 Conceptual confusion: chain or network?

Researchers frequently refer to networks, whereas official government documents in the Netherlands use the terms 'supply chain' (*keten*) and 'supply chain management' (*ketenbenadering*). They do so even when the term 'network' would seem to be more appropriate, considering the application being discussed.

In supply chain management, organisations and actors work together to solve a problem or reach a certain goal. The links in the chain are not imposed from the top down by an overall authority; instead, they are driven by the needs and requirements of the various organisations for one another's product or information (Grijpink 2005). The supply chain is a linear process in which organisations work outside their own boundaries to achieve a common result (Borst 2009). The sequence of actors in the supply chain is determined by the problem that needs to be solved or by the product or service that must be delivered. Each actor is needed for the supply chain to work properly.

In addition to supply chains, organisations in both the public and private sectors are increasingly connected to other organisations in networks. The term 'network' refers to a relatively open association in which various 'nodes' are linked to other nodes through multiple, transverse and often redundant connections. Information moves from node to node along these connections (Barney 2004). Unlike supply chains, networks offer various alternative paths to information-sharing. Information can move in one direction, in different directions simultaneously, in reciprocal directions, and along multiple branches. Connections can also be strong or weak, single or multiple. The dynamic, flexible and adaptive nature of a network makes it difficult to coordinate and control (Castells 1996). Although on paper every information flow in government is regulated – information does not 'flow freely' but along pre-determined routes defined by law – and the term 'supply chain' is therefore a good description, things often turn out different in everyday life, and the actual dynamics are closer to a network. By referring to supply chains instead of networks in such cases, government is not properly acknowledging the complexity of the information flows.

In addition, government is also investigating the emancipating effects of ICT in the service, care and control sectors: digital service delivery must become more 'citizen-centric' (Citizen Service Card, Citizen Service Number), ICT should liberate patients and allow them to live independent lives for as long as possible (Keizer 2011), and the police are calling on the public to use their mobile phones to help with their surveillance and enforcement work.

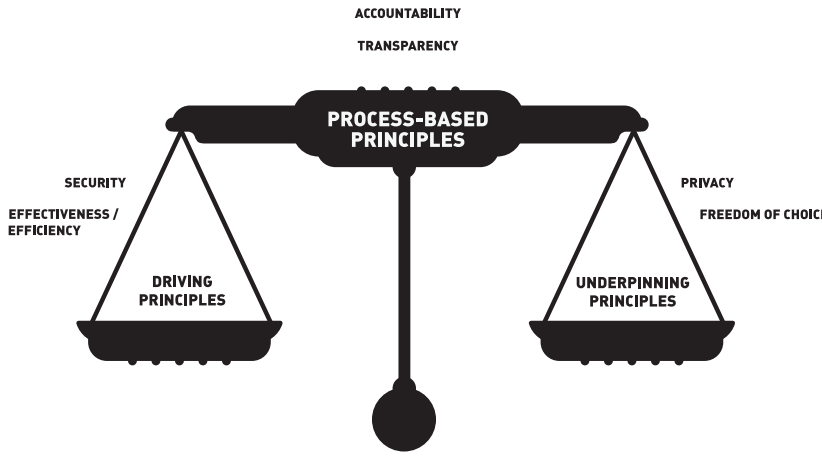
The analysis in Part II shows that innovations in digital service delivery are also providing new ways to observe and control citizens. In other words: without bureaucracy, no Big Brother – but also no welfare state. Some of these innovations illustrate that the boundary between service, care and control is becoming increasingly blurred, and the Netherlands is not alone in that respect (Lips, Taylor &

Organ 2009). When filing cabinets are converted overnight into digital databases that can be interlinked and allow for remote, rapidly executed searches, new forms of collaboration become possible. That is true for digital service delivery, digital care and digital control. According to Lyon (2007: 3), government surveillance of citizens always takes place somewhere on the continuum between care and control. Various authors point out that bureaucratic record-keeping can be both an instrument of control and an instrument of distributive justice (see e.g. Lyon 1994; Marx 2001; Gilliom 2001). But there are other reasons why it may be difficult to make a sharp distinction between control, service and care. Whereas Foucault (1977) referred to the 'disciplinary society', which emphasises disciplinary institutions such as prison and school, his philosophical 'heirs' such as Deleuze (2002) refer to the 'society of control', in which control has become a permanent process disassociated from physical location and, as a result, from institutions. It is precisely this change that can lead to shifts in the boundaries between the various roles of government in its everyday relationship with citizens (service provider, controller, carer), causing categories such as service, care and control to overlap.

2.4 THREE GROUPS OF PRINCIPLES: AN ANALYTICAL TOOL

In discussions on the development of various applications – such as the Electronic Patient Dossier, the biometric passport, and the public transport chip card – the relevant actors put forward all kinds of different evaluation criteria, including security, transparency, and freedom of choice. They do so for various reasons: to support a digitization proposal, to limit or extend its impact, or to promote sound procedures for the normal use of an application. In this book, we refer to such criteria as 'principles' and analyse them as such. These are the principles against which developments in ICT are measured, both in this analysis and by actors in the field. Throughout the development process, actors advocate a range of principles. The form an application ultimately takes – not the technology alone, but also its social (administrative, legal) context and impact – is the outcome of a struggle between the ideas and normative positions brought into play, many of them conflicting ones. Our empirical analysis would get bogged down in detail and contradictions if it examined every principle in turn. That is why this book examines *three clusters* of principles, which are more relevant to our analysis than the individual principles themselves. This tripartite division distinguishes between driving, underpinning and process-based principles. It helps clarify what are often complex arguments about criteria by dividing the most relevant principles into three categories, which then provide a basis for our analysis. What everyday experience has in any event made absolutely clear is that the effective use of ICT in the relationship between government and citizen requires choices to be made. After all, it is ultimately impossible to do justice to all of the principles that come into play, as important as each one may be.

Figure 2.1 Diagram of tripartite division of principles



Driving principles are those related to government's drive to utilise ICT in all kinds of domains. The driving principles focus on improvement and quality gains. We will look in detail at two principles that are frequently raised in the course of discussion: *security*, and the ostensibly interlinked principles of *effectiveness* and *efficiency*. Underpinning principles have to do with guaranteeing rights and freedoms, charting 'silent losses' as the process of digitization unfolds, and protecting the autonomy of the individual. They constitute a counterbalance to the driving principles and rein in their power. *Privacy* and *freedom of choice* are two important underpinning principles analysed here. In order to arrive at a well-balanced application or sound decision relating to the use of ICT, principles need to be compared and contrasted. Process-based principles provide the procedural framework that makes a balanced comparison between driving and underpinning principles possible. The process of balancing these principles must be open and verifiable. This study therefore considers the process-based principles of *transparency* and *accountability*.

It is important to note that these six principles do nothing more than operationalise the categories of the tripartite division. While they all play a prominent role in the dynamics of government's use of ICT, they do not offer us an exhaustive picture. They do provide a very realistic illustration, however, of how driving, underpinning, and process-based principles are compared and contrasted, making the analysis less abstract. There are naturally other normative concepts that play a role in the thinking about ICT and government, for example accessibility, legitimacy, legal certainty and equality. It is impossible to compile an exhaustive list of individual principles or to offer the ultimate description of them, if only because the information society is in a state of permanent evolution.

Categorising principles in this way shifts the emphasis to the *process of balancing* different – and dissimilar – normative principles adopted by the Government and Parliament (among others) when a new technology is introduced. Each time, assorted, and often opposing principles – for example privacy, transparency, and security – must be compared, contrasted, and balanced. Comparison is not based on individual criteria, in any case. After all, an analysis that looks solely at the driving principles – with everything boiling down to the gains that ICT will or will not produce – can all too easily disregard the softer values (Nussbaum 2000) that may be at stake, or the process-based, democratic nature of the innovation (Shrader-Frechette 1992: 131). This study therefore focuses less on the individual principles themselves and much more on their normative character and how they influence the debate about ICT. In other words, our analysis looks at what the principles *do* (how they influence developments and discussions), and not at what they *are* (as concepts and in terms of content). Part II analyses how these principles are interpreted in practical terms, within various policy contexts. Comparing dissimilar principles requires a different approach to that used by such bodies as the Netherlands Court of Audit, which assesses ICT projects in terms of efficiency and lawfulness or the Office of the National Ombudsman, which applies various adequacy criteria when analysing government performance. The approach taken here also differs from the normative criteria that researchers have proposed for ICT use, for example Franken's *General principles for proper ICT use* (Franken 1993) and Bovens' *Information rights* (Bovens 2003). Comparing dissimilar principles is a different type of exercise to satisfying a relatively exacting list of criteria.

The following sections discuss driving, underpinning and process-based principles in turn. We begin by describing the nature of each of the three categories and its function. Secondly, we briefly consider specific principles in each of the three categories, allowing us to raise various points about the process of comparing and contrasting driving, underpinning and process-based principles before moving on to the empirical analysis in Part II.

2.4.1 DRIVING PRINCIPLES

Electronic government is undeniably dynamic. ICT drives government's ambition to create new opportunities for policy. At the same time, some of government's aims – to improve service delivery and security – dovetail seamlessly with the new opportunities offered by ICT. And this is not happening in the Netherlands alone: many Western nations are pursuing a client-friendly, proactive, efficient eGovernment that uses every electronic tool available to optimise security and service delivery. They are meeting with little resistance in that regard. After all, who is going to oppose better quality and more effective government? In practical terms, driving principles are self-evident.

Technological advances, for example in the area of security, and the promise that ICT will improve effectiveness and efficiency demand that government reap the benefits of such innovations. The pressure to utilise technology is enormous, and not without good reason. Among politicians and policymakers, the progressive, dynamic nature of ICT is almost its own motivation. ICT brings success within reach, and any further justification is virtually unnecessary, thanks to the promise technology holds out for the future and the optimistic view of it described earlier. The apparent ease with which technological solutions are accepted also means, however, that the driving principles are taken for granted in discussions and have therefore hardly been crystallised in any real sense. Because no one evidently opposes more effectiveness and efficiency or improved security, very few questions are raised about these principles. Their dominance in public and policy debates means that they often overshadow other interests. Driving principles are therefore certainly not endangered in everyday life. Indeed, the biggest difficulty lies in conducting a credible, broad, normative assessment that encompasses other principles as well.

Effectiveness and efficiency

We have already said that driving principles are often left out of any normative analysis but in fact attract a great deal of attention in everyday practice. One good illustration of this is how the terms 'effectiveness and efficiency' are used in discussions about applications. Effectiveness can be defined as the ability to meet pre-determined targets. Efficiency is often defined as the attainment of a specified target using the fewest possible resources. An improvement in efficiency implies achieving 'the same' (the pre-determined target) with 'less' (time, effort and/or money). Even though effectiveness and efficiency stand for two different things, they are often mentioned in the same breath when it comes to government service delivery. ICT's ability to serve both purposes hides any contradictions, for example the fact that efficient policy can be highly ineffective.

The problem with embracing effectiveness and efficiency mainly in the rhetorical sense by regarding them as an automatic and permanent feature of ICT initiatives becomes apparent when such initiatives are evaluated. Because we lack a good definition of what effectiveness and efficiency entail and how they are to be measured, it becomes difficult to determine whether targets have been attained. Evaluation is – or in any event should be – a vital component of the learning (high-tech) government. In policy discourse, however, effectiveness and efficiency are often put forward or assumed as 'knock-out arguments': merely claiming that something is effective and efficient is seemingly enough. There is often no real validation of the claims made within the context of eGovernment, as we will see in Part II.

Effectiveness and efficiency have always been hugely important in government, but they have come to play an increasingly important role thanks to the influence

of ICT. This is because performance indicators, forceful action, and forms of 'management by objectives' have gained leverage in both the private and public domains. For example, the political discussion about the EPD focuses on the number of patients whose lives will be saved (Pluut 2010) and the success of the Reference Index for Juveniles at Risk (VIR) is measured by the number of risk reports (Keymolen & Prins 2011). The New Public Management philosophy focuses on such objectives as customer-friendliness, getting results, and working efficiently, propagating the idea that government should be reformed in accordance with the efficiency model. Although that idea has now been qualified, effectiveness and efficiency are still prominent items on the public management agenda (De Groot 2010).

The policy documents and reports on eGovernment that have been published in recent years show that improvements in the effectiveness and efficiency of government performance were the most important drivers behind the development of eGovernment (Snellen 2005: 399-400; Bekkers & Homburg 2009). However, it is dangerous to summarise the metamorphosis that ICT has wrought in government organisations with the 'more with less' mantra because that ignores the fact that ICT has also changed government itself. ICT-driven government is not – or not only – more efficient government: it is *fundamentally different* government.

Security

Although it differs from effectiveness and efficiency, security is also a driving principle. Security has become a dominant policy objective nowadays. Like effectiveness and efficiency, it is beyond question – security is, after all, one of the state's *raisons d'être* – but it is also a highly dynamic, transformative principle. Not only has the threat of international terrorism focused political attention on the principle of security, but the nature of our 'domestic' need for security has also changed dramatically. Government is increasingly expected to identify and manage risk, preferably before it develops into an actual threat (Beck 1992; Boutellier 2003; WRR 2008b). This pattern of expectations requires government to switch from reactive to proactive, from repressive to preventive, from criminal law to a comprehensive 'governance of security' (Johnston & Shearing 2003; Schinkel 2009).

ICT is playing a huge role in this transition. We already know that there is a connection between ICT and the rise of the 'society of control'. Information technology has specific implications when it comes to recording the behaviour and actions of citizens: observation has become more intensive, all-encompassing and invasive. Digitally recorded images and data are also available for a much longer period of time than personal observations (by police officers, social services investigators, etc.). This chapter has already raised the point that digitization offers new

opportunities to access, share, and enhance information. In terms of detection, public order and crime control, therefore, ICT has a range of advantages.

Security has been the driver behind many trends and innovations in ICT and government. Although these innovations have not led to a 'Big Brother' scenario, the fact that Big Brother is referred to regularly in publications and debates shows that policy initiatives taken in the interests of security tend to be quite expansive. That tendency to expand is also evident in other forms of control not strictly dictated by security policy. The increased priority given to law enforcement and the assessment of lawfulness, for example with respect to the public funds spent on social insurance schemes ('checking behind your front door'), is an exponent of the same drive for control, a drive that has been greatly facilitated by ICT. One good illustration is Automatic Number Plate Recognition (ANPR). This camera technique is used by the police to enforce public order and investigate crime, but it is also used by the Ministry of Infrastructure and the Environment to monitor waste transport, by the Transport and Water Management Inspectorate to check on transport by taxi and whether taxi drivers are taking proper breaks, by RWS (*Rijkswaterstaat*, the executive arm of the Ministry of Infrastructure and the Environment) to control traffic flows, and by the Tax and Customs Administration to check up on various taxes (Tweede Kamer 2009-2010j).

The expansive nature of control manifests itself in many contexts as 'function creep'. The network-like nature of information technology makes it exceptionally tempting to add control functions to all kinds of systems that are basically intended for other purposes, or to link systems to other systems that have a control function. For example, during a debate in the Dutch Senate relating to a bill to introduce an 'alcohol lock' in cars, questions were raised about the relationship between the system for registering drunk drivers (by the Central Office for Motor Vehicle Driver Testing and the Centre for Vehicle Technology) on the one hand and the Electronic Patient Dossier on the other: "Does the Government foresee an eventual link to the Electronic Patient Dossier, owing to the potential relationship between alcohol consumption, the use of medication, and a person's ability to drive?" (Eerste Kamer 2009-2010d: 4). The technical possibilities pave the way for function creep.

2.4.2 UNDERPINNING PRINCIPLES

Personal freedom and the limits to that freedom under a democratic system of government have long been a topic of debate in classical liberal-democratic philosophy. The freedom to be oneself, to be different to others, and to be so openly and in public view – within the boundaries of the law – is closely bound up with the very concept of citizenship (Van Gunsteren 2009: 42). The collective and individual core of freedom upon which government must not encroach is made up of underpinning principles such as freedom of expression, the freedom of the press,

and the right of assembly – but also freedom of choice and privacy. These underpinning principles provide a counterbalance to the techno-optimism and, often, overwhelming influence of the driving principles that accompany the introduction of technological applications in government. This book considers freedom of choice and privacy, precisely because the arrival of ICT has made the scope of these two principles a crucial topic of discussion.

As we already noted with respect to the driving principles, it is vital that government is given leeway to exploit the opportunities offered by ICT.[3] At the same time, however, the public must be protected against ICT's undesirable implications. Such protection can take different forms. For example, underpinning principles can be invoked to set absolute limits, in order to block the introduction or particular use of an application. Government could, for example, decide that facial recognition technology must be kept out of private hands (businesses and the public) because its widespread use could be socially disruptive. Underpinning principles can also set limits to the connections between certain systems. The question raised in the Senate about a link between the EPD and records on drunk drivers serves as a good illustration. In his reply, the Minister for Health said: "A link between the two systems will not be provided for" (Eerste Kamer 2009-2010e: 12). Although he did not say it in so many words, the Minister's reasons were based in part on the principles of privacy law.

In such situations, the underpinning principles are only discussed – if at all – in relation to specific technological applications. In everyday practice, they are applied in specific, real-life situations. And in legal cases, principles such as freedom of choice and privacy are often nothing more than 'weighty interests' – interests that, even if genuinely at stake, may not necessarily be the deciding factor (see Dworkin 1977). Underpinning principles are generally not all-or-nothing concepts in public and political debate; rather, they function as guideposts for discussion.

Freedom of choice

Anyone exploring the concept of freedom of choice (or autonomy) will conclude that this underpinning principle is omnipresent in the law – but at the same time impossible to pinpoint. Omnipresent because the age-old (liberal) principle that "everything that the law does not forbid is permitted" still serves as an important source of inspiration for our legal systems. And it is elusive because the concept does not offer individuals watertight guidelines for their actions. Nowhere in the law does it state precisely what 'freedom of choice' – a concept so important to personal development and to the democratic system of government (the 'free citizen') – actually consists of, or what arrangements or rules apply in more specific cases. Germany is exceptional in having a constitutional right to 'general freedom of action' (*Algemeine Handlungsfreiheit*) (e.g. Haratsch 2006), but even that clarion call has little meaning in practical terms.

The definition of 'freedom of choice' changes constantly, not least owing to innovations in ICT and technological applications. With a range of new media, software and services at their fingertips, people today are faced with a bewildering array of choices. Political and administrative efforts to liberalise telecommunications and healthcare, for example, are predicated on freedom of choice. And the citizen profile that fits such policies best is an emancipated individual who contributes to the good of all by going his or her own way. He or she is a critical consumer, thereby stimulating competition and paving the way for optimal price setting. In other words, choice is a crucial civic duty (Hurenkamp & Kremer 2005). This profile fits in well with the liberating potential of ICT. Freedom of choice here increasingly means freedom of information, or rather, the freedom to decide on one's own actions based on a wide variety of information and information-based services (Lor & Britz 2007). The question is whether people in fact really desire as much freedom of choice as they are given (or compelled to take). Simon (1956) and, later, Schwarz (2004), claim that many people in fact do not set much store by freedom of choice, or are not really able to make choices. Economic theory and social psychology have also explored the shortcomings of the 'rational choice model'. Because this particular view of human behaviour ignores many fundamental factors, "it would be better to simply accept that the rational choice theory is not always a suitable one for understanding the world" (Tiemeijer 2009: 328). In other words, freedom of choice is an important but rather elusive concept.

Privacy

Like all other traditional fundamental rights, privacy represents an individual 'space' in which government does not interfere, but this right also safeguards the conditions necessary for individual human development. The principle of privacy is firmly grounded in European constitutions. This has led, in part, to the notion that government must also guarantee that citizens respect one another's right to privacy (e.g. Verhey 1992; Fredman 2008), i.e. that privacy has a 'horizontal' bearing as well as a 'vertical' one. There is, therefore, no way around the fact that government bears final responsibility for the protection of privacy, not even in a world in which enormous commercial 'information monopolies' (Google, Amazon) appear to call the shots and the Internet seems to be beyond regulation. In addition, constitutional rights are frequently at odds with one another in real life, a situation aggravated by the fact that privacy is a difficult concept to define (see Blok 2002; Solove 2008). That is because in most situations, privacy is a question of weighing the various interests involved, and in many cases, individual rights end up taking a back seat to the perceived interests of the collective. It is therefore difficult to distil the core substance of the right to privacy from case law (e.g. Gómez-Arostegui 2005).

The meaning of privacy is changing constantly, if only because each successive generation views it differently. For example, the new 'generation' of digital natives

(Palfrey & Gasser 2008) seem to have different ideas about privacy (see also Boyd 2008) to the 'pre-Internet' generation. Mutual respect for privacy is a hot topic these days, and Internet applications such as Facebook have demonstrated that account holders are increasingly dependent on the providers of such services to protect their privacy. The advent of cloud computing also shows that people are coming to depend more and more on major commercial actors of unknown whereabouts and identity in their interactions with others and, consequently in the exercise of their right to privacy. "What happens to your family's photo collection if it's held in the cloud and your password goes to the grave with you? And what about your documents and emails – all likewise stored in the cloud on someone else's server?" (Naughton 2010a).

The meaning of privacy has always been shaped and adapted in response to new technologies, however, and the current era is no exception. For example, American privacy law has its origins in the rising popularity of photography at the end of the 19th century – or rather, it developed in response to that technology, with the tabloid journalist's camera being an important reference point. In a landmark article, Warren and Brandeis (1890) argued that an individual's right to privacy must be protected against the unregulated and threatening phenomenon of photography – an aim that they eventually achieved. Since then, we have increasingly come to interpret the 'space' that privacy law is designed to protect as informational. Departing from its traditional physical function (the sanctity of the home), the concept of privacy has evolved into a more intangible right, making it much harder to define absolute limits (Floridi 2005). At the same time, there are in fact very clear lines that can be drawn between the older physical concept of the sanctity of the home and the more non-physical forms of modern informational privacy. Specifically, it is the genuine human need for a certain degree of solitude (individual or collective) in order to nurture, develop, and keep one's person afloat – in other words, the need to shape one's own identity. In *The Human Condition* (1998, p. 71), Hannah Arendt expresses the genuineness of this need as follows: "A life spent entirely in public, in the presence of others, becomes … shallow. [I]t loses the quality of rising into sight from some darker ground which must remain hidden if it not to lose its depth in a very real, non-subjective sense." Further evidence that our understanding of privacy is adapted in response to new technologies can be found in the National Constitutional Committee's recommendation that privacy should be dealt with separately from personal data protection in the Constitution. According to the Committee, it was clear that "technological advances, European trends and developments and globalization have led in recent years to a dramatic rise in the volume of personal data that is being shared and analysed. Creating a separate right to protection of personal data would acknowledge that the use of such data has become much more important and that it is desirable to provide proper protection in today's society" (Staatscommissie Grondwet 2010: 81-82). All of the interest shown in the protection of personal

data in private relationships sometimes overshadows the traditional concern of protecting one's privacy and personal data against government (e.g. Levin & Sánchez Abril 2009). It remains a thorny question for government, which is accountable not only for its own use of ICT, but also for the way in which digital citizens deal with one another. After all, government cannot avoid bearing final responsibility for the way in which the information society deals with privacy (De Hert 2011).

2.4.3 PROCESS-BASED PRINCIPLES

Even if it is impossible to say in advance which set of principles – driving or underpinning – should prevail in a particular case, we can say a great deal about the quality of the conditions under which the balance is struck. The process-based principles – illustrated here by the principles of transparency and accountability – provide a framework for greatly improving the quality of the discussion on the development of eGovernment and the associated decision-making process. They play a decisive role in preserving a proper balance between driving and underpinning principles, but they are also important in the preceding process, when seeking and discussing that balance. They also guarantee the verifiability of the process by which electronic government develops. Together, transparency and accountability ensure that the comparison – often implicit – that government is obliged to make when introducing applications is clear, comprehensible and open to objection.

Process-based principles are valuable in that they subject the discourse of both driving and underpinning principles to a reality check at the macro level, allowing rhetoric to be separated from reality in policymaking. They are also valuable at the micro level whenever a policy outcome or a specific decision by a public body affects an individual citizen. If these principles are properly interpreted and laid down in institutional arrangements and rules, they can help correct errors and build in the feedback mechanisms required by a learning government.

Transparency

Citizens require two forms of transparency: (1) the kind that allows them to scrutinise the political and policymaking process and offer a counterbalance when necessary, and (2) the kind that makes it possible for them to exercise their individual rights in full. Transparency is therefore the forerunner of accountability in many respects.

The first form of transparency helps citizens understand the processes behind the policy and therefore delivers more complete and more accurate information to the public domain. This form has made great strides under the banner of 'active open government'. The Open Government Initiative in the United States is a good example, but there have been several similar projects in the Netherlands as well,

ranging from Internet consultations on legislation to the tweets of politicians and policymakers. Digital access to information has many advantages and very few disadvantages for citizens. Not only does it allow them to keep up with what is happening and remain politically engaged, but it also helps them act as a countervailing power in the political and policy arenas.

The second form of transparency relates to individuals who are seeking legal redress, offering them guidance in protecting their rights. People inadvertently caught in the tangle of digitized government need to understand what has happened before they can take steps to solve the problem. Owing to the specific nature of information technology, the old adage 'what you don't know can't hurt you' does not apply in many cases; indeed, if anything, what you don't know can indeed hurt you. So a certain degree of transparency in government's internal processes is necessary to reinforce the legal position of the citizen. Websites such as mijn.overheid.nl, burgerpolis.nl and mijn.belastingdienst.nl[4] show that government does in fact use ICT to furnish individual citizens with transparency, albeit with some reluctance. What is important, however, is the extent to which transparency offers individual citizens guidelines for legal protection. For example, the worrying quality of some government information (see e.g. Grijpink 2006; Choenni et al. 2011) and the growing problem of identity fraud raise the question of who bears the burden of proof when it comes to inaccurate information, and how that person can find out about it. Another key aspect of government's growth to ICT maturity is that it has so far been very concerned making citizens transparent for government, but has devoted very little attention to the contrary (Keymolen 2007; Prins 2007). However, the push to make citizens transparent (for the benefit of proactive policy, etc.) is dominated mainly by driving forces such as security, and has little to do with the process-based principle of transparency.

Accountability

The concept of accountability closely resembles the verifiability that is made possible by transparency, but adds binding consequences to the equation. In its political manifestation – for example parliamentary control and ministerial responsibility – accountability serves as an important test of government's performance and the way in which it has weighed up driving and underpinning principles. In its legal manifestation, accountability allows citizens to challenge the outcomes of eGovernment. If accountability is sufficiently provided for, citizens can do more than just speak up for their individual rights; the accretion of citizen actions produces a critical countervailing power that may help improve the quality of the relationship between government and the citizen in the digital age.

In addition to these more external (public) forms of accountability, a form has also emerged within organisations, i.e. an internal form, which can be described as

managerial accountability. This focuses mainly on control and governance (and learning processes) within organisations. ICT has changed the landscape of organisations dramatically in this regard. For example, expert systems now streamline and manage the work carried out by professionals, and the potential for record-keeping has increased enormously. Computerised logs make it possible to register and store every digital interaction. The records can be used to produce management information, which is then used for actual management purposes. One good illustration in this connection is the response of the Association of Dutch Municipalities to the draft bill for the Reference Index for Juveniles at Risk (VIR):

> "If, based on reports in the VIR, there are indications that a situation involving a juvenile is becoming unacceptable and those authorised to issue reports fail to take appropriate action when called upon to do so by the coordinating body, then it must be clear who is authorised in this case to take binding decisions on the necessary arrangements and issue instructions to social workers" (VNG 2008: 2).

The importance of accountability would be difficult to overestimate in today's society. In a time when a single, overarching governance philosophy seems doomed to fail given the complexity of society, a process-based principle such as accountability offers an alternative. It requires only that a relationship of control exist between a forum and an actor, permitting those whose interests are being represented in the forum to exercise some control over the actor in question. This emphasis on *operational control* demonstrates the systemic difference between the accountability mechanism and the more traditional institution of legislation. Legislation is an attempt to pin down social relationships and behaviour in advance, whereas the nature of the 'accountability' instrument is to monitor actual performance, the incidents as they unfold. As a result, accountability "now crops up everywhere performing all manner of analytical and rhetorical tasks and carrying most of the major burdens of democratic 'governance'" (Mulgan 2000: 555).

2.5 WEIGHING UP THE PROS AND CONS

A balanced development of iGovernment requires each of the 'clusters' of principles – driving, underpinning and process-based – to be given its due in decision-making. They must be weighed up against one another, although that does not mean that each of them should be regarded as equally important in every situation. But because these clusters are generally at odds, one must also bear in mind that each one, and each principle, is relative. Every principle is in danger of being overvalued or undervalued. We look generally at the dangers of such 'excesses' below. In short, it is not possible to indicate in advance what a 'good' comparison of principles involves in relation to ICT, or what effect it will have. When this

study refers to a 'balance', then, it is not implying that that balance can be prescribed outside of the relevant context. There is nevertheless a great deal that can be said about such comparisons, for example that those carried out by politicians and policymakers (including Dutch ones) are often inadequate, as described in Part II.

We will begin with the driving principles. They are self-sustaining, and in that respect there is little risk that efficiency, effectiveness and security will lack attention. Government can never be efficient or effective enough, of course, but there is a danger of these principles becoming overly dominant, with economic rationalism hedging in all the other concerns that people may have about the role ICT plays in the relationship between government and the citizen. The same goes for the principle of security: in theory, society can never be safe enough (let alone too safe), but the emphasis on security can also be too one-sided, i.e. the pursuit of security at any price. That 'price' may in fact be very high, and not only in economic terms: a society whose members are under constant surveillance will find it hard to live and breathe. Private life "increasingly resembles a glass house with hardly any curtains" (Kohnstamm & Dubbeld 2007). If the principle of security is underplayed, on the other hand, government could very well be accused of both naïveté and of neglecting its most basic responsibility to citizens.

As Part II of this report demonstrates, the underpinning principles are often overshadowed in political and public debate by the driving principles. Underpinning principles are not automatically taken into account in the process leading up to the development of an application. They require particular attention and powerful advocates. Nevertheless, what applies to the other principles also applies here: there can be *too much* freedom of choice or privacy (compare De Mul 2010). For example, giving people unbridled freedom to decide whether their personal data can be used (for example by police investigators) would ultimately undermine the safety of others. Too much choice can equally lead to 'choice fatigue', with people not even taking the trouble to consider other options and simply ticking boxes at random. But a society can also have an excess of privacy: the free citizens of a democratic state have duties and responsibilities as well as rights, and for that reason it must be possible to trace and identify them. Protection of privacy has its risks. Undesirable scenarios can unfold behind closed doors, making privacy a breeding ground for threats and hazards, for example. "In a democratic society, it must be possible to call people who violate the rights of others to account. That may require disclosure of an individual's identity and an investigation into his or her activities," according to the fourth Balkenende government (Tweede Kamer 2009-2010j: 12). And many other unwelcome situations can arise in the physical or mental seclusion of the cocoon protected by privacy law. Critics point to traditional patterns of (male) dominance (Tadros 2006; Allen 2003), to concealment that is damaging to economic life (Posner 1984), to suppression of the expression

of public opinion (Volokh 2000), and even to general intellectual poverty (Kumar 2004).

It is also possible to overemphasise the process-based principles. No matter how important transparency is, it cannot be made an absolute demand. For one thing, some matters are simply too sensitive to be disclosed publicly (for privacy or national security reasons). Transparency also has a complex relationship with the public's sense of trust in government. Although government can use transparency as a tool to encourage trust (Keymolen et al. 2011; Van der Hof & Keymolen 2010), too much transparency may in fact be at the expense of such trust (Luhmann 1979). Government can also use transparency as a manipulative tool (Fung, Graham & Weil 2007) if the disclosure is never verified in an appropriate forum (Meijer, Brandsma & Grimmelikhuijsen 2010). The term 'audit explosion' alone (Power 2005) indicates that a society can also go too far in terms of accountability. The price of excessive accountability may be effectiveness and efficiency, and creativity (innovation).

2.6 IN CONCLUSION

The analytical framework presented above, the theoretical background to the main issues, and the tripartite division of principles will help to illuminate our analysis of the practical, everyday reality of eGovernment presented in Part II. That reality reveals that the nature of government is changing dramatically under the influence of digitization. A *de facto* practice has developed – virtually unnoticed – in which interrelated information flows dominate the character of government. That practice has not become part of the mental framework of politicians and policymakers; in fact, the overall idea of fast-expanding and rapidly diversifying information flows is virtually the last thing driving the way they think and work. In the meantime, information is cascading between different organisations, between what were formerly separate sectors (service, care and control), and across public-private boundaries. The empirical analysis in Part II follows the path of the information flows rather than the individual technologies and applications, and shows that in practice, iGovernment 'emerges' without needing to be 'engineered' by politicians and policymakers.

NOTES

1 www.bof.nl/2010/09/22/geen-openheid-over-nederlandse-blokkade-verboden-websites/

2 They include work and income, tax and customs, education, traffic and transport, etc.

3 And also so as to not unnecessarily prevent society (the market) from exploiting those opportunities.

4 Roughly translated: my.government.nl, citizenpolicy.nl and my.taxandcustoms.nl.

PART II

EMPIRICAL ANALYSIS

3 MANAGING eGOVERNMENT

The previous chapter explains that this study focuses more on technological systems in relation to their environment than on individual technologies or technology in general. Such sociotechnological systems consist of complex networks of people, technological applications, government and other organisations, and businesses. The motives and interests of the actors involved play an important role in charting the course that technological development takes and in generating and utilising information. The interactions that take place within this sociotechnological system are therefore the point of departure for the empirical analysis set out in this part of the book. That analysis zooms in on the relationships between the key actors that shape eGovernment, revealing how they go about taking decisions on the use of technology and information and balancing interests that are often contradictory, as well as the role that each actor plays. Their positions are subsequently defined in terms of the driving, underpinning, and process-based principles introduced in the previous chapter. In analysing the interactions between them, this study not only looks at technological applications, but focuses in particular on the information flows that arise from or are facilitated by technology. It is in such information flows that the boundaries – which are already somewhat blurred – between various policy areas, regulatory chains, sectors, and the relevant parties tend to converge. Focusing on information flows reveals the outlines of the quiet revolution in eGovernment – a revolution that will determine the future and the character of government in the digital age.

3.1 THE ENTHUSIASM AND 'TECHNO-TRUST' OF POLITICIANS AND POLICYMAKERS

3.1.1 READY AND WILLING

On 21 June 2001 – not long before the terrorist attacks in New York – the Dutch House of Representatives discussed the Dutch Minister of the Interior's memorandum urging the inclusion of a biometric feature in travel documents, as well as a recent visit by several MPs to the passport producers, Royal Joh. Enschedé and the state printing and publishing company SDU. The Minister and the MPs were equally enthusiastic.

"After the visit to Royal Joh. Enschedé and SDU, Mr Zijlstra (Labour Party/PvdA) showed himself to be deeply impressed by the advanced features and immense potential of biometrics. … Mr De Swart (Liberal Party/VVD) was also impressed by the potential of biometrics after his visit to Royal Joh. Enschedé and SDU. In particular, exceptional progress had already been made on the finger-

print scan and iris scan. . . . The Netherlands should perhaps consider adopting a role as trail-blazer and become the first country in Europe to introduce biometric features. . . . Mr Balkenende (Christian Democrats/CDA) found the technical possibilities and advances most impressive after his visit to SDU and Royal Joh. Enschedé. The Christian Democrats believe the inclusion of biometric features . . ..to be urgent and pressed for quick action to be taken. . . . Mr Balkenende observed that inclusion of a biometric feature would require amending Article 3 of the Passport Act. This was a technical improvement, not a change in principle . . .” (Tweede Kamer 2000-2001a: 103).[1]

These passages, taken from the minutes of the meeting, illustrate the attitude toward ICT that has prevailed among politicians and policymakers in the past decade. That attitude is coloured by (a) huge enthusiasm and almost absolute trust in ICT and (b) an instrumentalist view of what ICT is and can do. The policy plans developed since the early 1990s all convey huge trust in ICT as a tool with which government can execute its tasks more effectively, become more client-friendly and more accessible, improve in quality, and prepare more thoroughly for the future (see for example Ministerie van Economische Zaken 1994; Ministerie van BZK 1998; Ministerie van BZK 2000; Ministerie van SZW 2010). ICT was greeted with excitement by Dutch politicians, who thought it would help government shoulder its heavy administrative burden and allow it to tackle urgent social issues such as terrorism, security, mobility, and good and affordable care. It was virtually taken for granted that technology would be used. Two communications about the national Electronic Patient Dossier, sent to the House of Representatives by the then Minister of Health Hans Hoogervorst, are revealing.

“In this memorandum, I have not discussed the necessity of introducing the Electronic Medical Dossier (EMD) and the EPD. After all, everyone is convinced that both must be implemented as quickly as possible” (Tweede Kamer 2004-2005: 8).

And:

“The second conclusion is that it is beyond doubt that the introduction of a GP observation dossier and the electronic medical dossier will improve the quality of care” (Tweede Kamer 2006-2007: 4).

Technology is ‘rolled out’, practices are ‘streamlined’ and services are ‘updated’. For example, the ICT applications developed by the Ministry of Security and Justice within the context of the Border Management Innovation Programme ensure that border surveillance strikes a good balance between the need for control

and security and the economic benefits of ensuring the efficient and customer-friendly handling of cross-border movements of people and goods.[2] A policy document published by the Ministry of the Interior and Kingdom Relations, *Contract met de toekomst (*Contract with the Future, Ministerie van BZK 2000), which looks ahead to government's electronic relationship with the citizens, also expresses high hopes for the problem-solving capability of ICT.

"ICT is more than merely a handy tool for improving efficiency. When properly used, it can make an important contribution to achieving the policy targets that a sector has set itself. It can oil the machinery of justice, in the same way that it has greased the wheels of the Tax and Customs Administration. It can help compensate for the shortage of teachers and remedial teachers in education, vastly improve the quality of life of the elderly, and make our streets a much safer place to be. The opportunities are there; we have only to grasp them. Understanding what ICT can do for a sector requires the involvement of experts from that sector. They know enough about the primary process to see what ICT can contribute. It is therefore important to get the sectors thinking about the problem-solving potential of ICT" (Ministerie van BZK 2000: 23).

3.1.2 FROM SERVICE DELIVERY TO CARE AND CONTROL

At first, the appeal of new technological innovations lay primarily in their potential to improve service delivery. eGovernment is "government in which transactions between government and the citizen take place as much as possible through electronic channels, the purpose being to improve service delivery and law enforcement and to encourage public participation and input by citizens. . . . The interests of the citizen are the basic point of departure in this respect" (Postma-Wallage Committee 2007: 4). It was this aim that inspired Dutch politicians to embark on a digitization campaign in the 1980s and 1990s. They sought to improve policy – doing more with less, so to speak – and streamline transactions between government and citizens by zealously digitizing administrative processes and by launching popular projects such as the Citizen Service Card and the Government Service Desk 2000 (Van de Donk & Meyer 1994; Huydecoper et al. 2001; Bekkers et al. 2005; Van de Donk & Van Dael 2005). And yet, when the Ministry of the Interior and Kingdom Relations asked the Public Administration Council (*Raad voor het openbaar bestuur*, Rob) to advise it in 1998, the Rob responded by observing that government had disregarded many opportunities to utilise ICT to improve service delivery to citizens. In its opinion, the projects launched within the context of the Government Service Desk 2000 project were "mere finger exercises for the major work that lies ahead" (Rob 1998: 23).

And indeed: a few years later, policymakers and politicians embarked on that major work in earnest. In *Contract met de toekomst*, the policy document cited

earlier (Ministerie van BZK 2000), the Government set out an ambitious plan to use ICT to improve both its data management and service delivery to the citizen. Whereas the early days of eGovernment saw greater emphasis on advancing a vision of 'new government', the accent now shifted to translating the aims (often imposed top down) into specific programmes and agreements. One such example was the 2008 National Implementation Programme on Service Delivery and eGovernment (*Nationaal uitvoeringsprogramma betere dienstverlening en e-overheid,* NUP), an agreement in which the national, provincial and local authorities undertook to improve service delivery while reducing the administrative burden. "In order to do that, the public authorities must cooperate (even) more closely, coordinate their operations and data management, and align them with existing and future basic facilities."[3] In the past decade, that idea has resulted in a wide range of plans and specific initiatives: the introduction of the Citizen Service Number (BSN), the modernising of the municipal personal records database (GBA) and various other basic records, the expansion of the intermediary organisation for electronic data-sharing between government organisations (RINIS), the establishment of a single client contact centre for income-support benefits schemes, and the many online facilities for administrative transactions (e.g. applying for a permit, submitting a notice of objection).[4] These and countless other initiatives have changed government service delivery in various ways (services are now continuously available, for example, and more interactive) and in some cases did indeed improve it. The celebrations, however, were often short-lived: improvements in service delivery are quickly perceived as 'status quo' and not as an achievement. Moreover, the 'silent' successes attained by local authorities and many government agencies are frequently overshadowed by more prominent, large-scale, expensive projects plagued by delays and failures.

The major work identified by the Rob was not restricted to service delivery. 'The Hague' has also increasingly turned to technology in the past decade to solve pressing social problems. That is partly because politicians have had so much trust in technology as a tool for tackling such problems more efficiently and effectively, but it is also because they have become increasingly interested in public safety, national security, and other issues in which technology plays a growing role. The Netherlands is certainly not alone in either respect (Lyon 2007; Dunleavy et al. 2006; Monahan 2006; Zureik & Salter 2005; Bennett 2008; Magnet 2009). ICT has become increasingly prevalent as an element of public safety policy in recent years: security cameras provide 24-hour surveillance on the streets, the Reference Index of Juveniles at Risk (Verwijsindex Risicojongeren, VIR) and the Electronic Child Dossier (*Elektronisch Kinddossier*, EKD) are meant to alert the authorities to young people at risk at the earliest possible stage, and databases of fingerprints and DNA markers make crime investigations easier. There is virtually a 'technological imperative' in place when it comes to national

security, with security-related data-gathering reaching unprecedented proportions. For example, Dutch crime investigation services requested customer data from telecom companies and ISPs almost 3 million times (2,930,941 times) in 2009 (CIOT 2010a). In addition, the Final Report of the CIOT[5] Audit – published after a request was submitted under the Government Information (Public Access) Act (*Wet openbaarheid van bestuur*, WOB) – revealed that the staff of special crime investigation units had requested such data without first obtaining the consent, required by law, of the public prosecutor (CIOT 2010b). It is anyone's guess, however, just how much data is gathered in other contexts. "Everyone knows that requests for data have increased considerably in recent years, but substantiating figures are only partially available" (Advisory Committee on Information Flows Security 2007: 66).

3.1.3 DRIVEN BY AMBITION

Politicians and policymakers are not only enthusiastic about ICT and have great faith in its powers; they are also ambitious. The Netherlands Court of Audit (2007a) refers to "an enthusiasm for ICT" among policymakers, unrealistic political deadlines, and insufficient scope for review and re-evaluation during projects. In the Court's view, ICT projects in national government are overly ambitious and too complex, the result of constant tension between the political, organisational and technical factors involved. The Coordinating CIO (see also Section 6.3), Maarten Hillenaar, has also remarked on government's inclination to embark on large-scale projects (a propensity not limited to the Netherlands alone), with 'fantasy deadlines' – for example to get a project up and running within the current Government's term in office – and the compulsion to build things from scratch, meaning that the mistakes of previous projects are repeated over and over again. Politicians are also frequently inclined to make changes halfway, influencing the scope of a project.[6] In addition, the politics of large-scale projects are often 'all or nothing': the Government is loath to see such projects fail, or even be delayed. For example, in response to the 330,000 objections lodged against the EPD – an unprecedented figure, and one that increased by another 100,000-plus by mid-2010 – Abraham Klink, Minister of Health, had nothing more to say than that that number is "in line with what he'd expected" (Pluut 2010: 21). Nevertheless, the EPD project has for now come to a halt. In April 2011, the Senate unanimously rejected the legislative act that would have constituted the national interchange[7] – thereby ironically relegating digital medical dossiers to regional public-private initiatives, which are thriving but far more 'unruly' in character.

Such grand ambitions are apparent not only due to the scale and complexity of the projects, but also the result of policy goals specified in the plans. Charged with the task of protecting public safety and confident that technology is just the thing to

do the job, politicians want to map out and anticipate the future. "The technical system must ban uncomfortable uncertainty" (Hirsch Ballin 1992: 77). In keeping with the idea that prevention is better than cure, ICT is making it possible for government to act proactively and preventively (Schinkel 2009). The VIR must prevent the abuse and death of yet another child; the EPD must protect patients against medical errors; European migration databases must prevent more irregular migrants from entering the Netherlands; and investigation databases and the sharing of Passenger Name Records[8] and bank and DNA data must prevent new terrorist attacks. The yearning of politicians and policymakers to anticipate the future is leading to fundamental paradigm shifts. For example, the aim and scope of criminal law has shifted from response, revenge and rehabilitation to prevention and risk management or to the 'pre-crime logic of security' (Zedner 2007; Koops 2006; Teeuw & Vedder 2008; Buruma 2011). Garland (2001) refers to a 'culture of control' and describes a political climate in which fighting crime no longer means resocialising those who exhibit undesirable behaviour, but rather protecting people who adhere to the rules from those who do not.

3.1.4 ACCUMULATING BIT BY BIT

Driven by their enthusiasm for technology, their trust in its potential, and their ambitious aim of using ICT to tackle the challenges facing society, and spurred on by such principles as security, effectiveness and efficiency, politicians are eager not only to use separate applications but also to link and share information. If it is possible to uncover fraud by linking the information systems run by the Tax and Customs Administration and the Social Security Agency, there must be leeway to do so. If a child can be saved by giving as many organisations as possible access to the Electronic Child Dossier, then that possibility must be considered. If the fingerprints of asylum-seekers recorded within the context of migration policy can also be used to investigate crime, then what objection can there possibly be? If it is possible to share DNA data with the authorities in other countries by making national databases mutually accessible, then we'll sign a treaty to that effect. And, if screening Internet data traffic using deep packet inspection (DPI) makes it possible to stop the distribution of child pornography, it should be regarded as a serious option.

The growing desire to link systems and databases demonstrates that, although technology dominates the political debate, the issue is really the information flows facilitated by the different technologies. Information is the raw material of preventive policy because the profiles used as a basis for risk analyses and prevention can only be compiled with the help of information (i.e. personal data) (Harcourt 2007; Hildebrandt & Gutwirth 2008; Buruma 2011). Information is also the primary raw material within the context of a 'service-oriented' policy on poverty, for example when certain groups of citizens are excused from paying

their municipal or water board taxes, or are given access to supplementary benefits (Tweede Kamer 2009-2010b). Government also frequently 'shops around' in private databases for the information it requires. Increasingly, the public authorities require data gathered in the private sector for reasons of commercial service delivery to be made available to government – where it is for control purposes rather than for service delivery. Berkvens (1992) refers in this connection to the 'New Feudal Services' in the digital domain. The past decade has seen a string of new laws that make this possible, including the Requisitioning of Data Powers Act (*Wet bevoegdheden vorderen gegevens*), the Requisitioning of Telecommunications Data Act (*Wet vorderen gegevens telecommunicatie*), as well as European legislation relating to the transfer of passenger name records (PNR) and bank data (SWIFT) to the United States. In addition to such major public-private information flows, however, legitimised by special legislation, much can also be achieved by merging data resources from the bottom up. For example, if a municipal social services department wants to track down people committing benefits fraud, the Personal Data Protection Act (*Wet bescherming persoonsgegevens*, WBP) basically permits it to link its files with those of the water supply company (CBP 2006: 1). In all such cases, the cumulative use of information blurs the boundary between service (in this case provided by the private sector) and control (public sector). On the other hand, the private sector is happy to hitch a ride with government. As the Confederation of Netherlands Industry and Employers (VNO-NCW) has explained: "The Confederation is worried about the fact that, until now, opportunities to use the Citizen Service Number (BSN) in business record-keeping have been lost" (VNO-NCW 2005). And The Centre of Expertise (HEC, a public ICT consultancy firm), when asked to advise on a request for funding submitted by the Immigration and Naturalisation Service in connection with a computerised passport control system (No-Q), concluded that "The objectives can be regarded as realistic given the firm commitment of both government and the private party, Schiphol Airport."[9]

As a rule, however, politicians do not focus on the interaction between various applications and information flows; instead, they concentrate on individual initiatives and discuss them separately. For example, there have been parliamentary and other political debates on the biometric passport, the public transport chip card, the BSN, DigiD, the digital client dossier (DKD), the electronic learning dossier (ELD), the Electronic Patient Dossier (EPD), the Reference Index for Juveniles at Risk (VIR), and the Personal Internet Page (PIP). All these debates concerned a specific, relevant technological application. And depending on the dynamics of the debate, the focus may even narrow to a specific aspect of the application. The debate on the public transport chip card, for example, centred on the 'hackability' of the chip (Van Eeten 2011). When the then Minister of the Interior and Kingdom Relations, Guusje ter Horst, was asked about setbacks in introducing the National Civil Service Smartcard, she indirectly provided evidence of this narrowing of

focus, stating, "We have received repeated reports that the technology may not be as safe as we had thought and hoped, and so we have repeatedly had to take extra measures" (Tweede Kamer 2008-2009c: 3). Only rarely does anyone involved in public or political debate mention the underlying web of interests and relationships that will arise or continue to expand. There is frequently no discussion of the reciprocal relationships, the links, and the chain computerisation that evolve in the background of individual applications and that are moulded in everyday practice, step by step. Whereas individual applications are often subject to parliamentary debate and intervention (although sometimes not until very late in the process, for example in the case of the EPD and the VIR), that is scarcely ever the case when it comes to the links between systems (as distinct from applications). Because many of these links are assumed to be legitimate under the generic regime of the Personal Data Protection Act (*Wet bescherming persoonsgegevens*, WBP), decisions about them are virtually never discussed openly or at the political level. The only 'assessment' is the obligation under the Act to notify the Data Protection Authority (*College Bescherming Persoonsgegevens*, CBP), and even then, the Authority only scrutinises notifications in exceptional cases. A search through the Authority's online database of notifications shows that many links have been created at the operational and municipal level without giving cause to any visible attempts at scrutiny or debate.

The tendency to gather more and more information while politicians frequently narrow their focus to the application and the relevant legislation means that the resulting links and information flows are growing wider and more complex all the time. Increasingly, information gathered for service, care or control purposes is also used, linked and processed outside those contexts. One typical example of how systems initially intended for service delivery are later used for surveillance and enforcement is the Minister of Justice's programme to set up a national database of prostitutes based on the Municipal Personal Records Database (GBA).[10] When the Ministry requests a person's name and address for its national database, a note is appended to that individual's GBA record that data was forwarded to the prostitution database. Because information cannot be removed from the GBA (the system does not overwrite a record when information is amended; it simply appends the new data), public servants in the civil records department (whose jobs mainly involve service delivery to citizens) will be able to see not only that someone is now a prostitute, but also that that person was a prostitute at some point in the past. Policymakers and politicians in fact seem unaware of the far-reaching consequences of this growing accumulation of interlinked, multi-contextual applications. And when Parliament does comment that an initiative "has or could have more far-reaching consequences than initially intended when introduced" (Eerste Kamer 2006-2007: 1), the relevant ministry generally fails to respond.

3.1.5 A LACK OF CRITICISM

This is not to say, however, that Parliament's input is insignificant. Both the Senate and the House of Representatives – but the former in particular – have been critical of the Government's ambitions. At times, the Senate has even accused the Government of side-lining Parliament in advance by not setting out such issues as the assessment framework and criteria for deploying an application in the relevant Act, but rather in an Order in Council (*Algemene Maatregel van Bestuur*), as was the case with the introduction of the BSN (Eerste Kamer 2006-2007: 1-2). Parliament's criticisms sometimes have the backing of organised groups of citizens and NGOs (see Section 7.2) campaigning for stricter democratic supervision in a growing number of policy areas in which ICT is deployed (Eijkman 2010; Prins 2010a). The Rathenau Institute (an advisory body to Parliament on science and technology) has also helped shape political opinion in various reports to parliament and other studies (Rathenau 1998; Rathenau 2008: 18; Rathenau 2010: 18-19). The Senate has been particularly receptive to input of this kind and has come to different conclusions than the House in a number of cases. For example, the Dutch Consumers' Association played a major role in getting the Senate to reject a bill relating to a smart energy meter in April 2009 (Eerste Kamer 2008-2009a; Cuijpers & Koops 2009). After severe criticism by the Data Protection Authority (CBP 2007) and other organisations, the Senate cut the period in which Internet Service Providers (ISPs) are obliged to retain records on their customer's data traffic from the 12 months approved by the House to a maximum of six months. The House had itself already reduced the data retention period from the 18 months proposed by the Government. The EPD dossier turned out to be so complex that the Senate convened a number of expert sessions to aid it in reaching an informed opinion, thereby doing justice to its sobriquet *Chambre de reflection*. In the end, it was the Senate that rejected the bill relating to the EPD in April 2011. And finally, in May 2011 the Senate decided to hold a policy debate in the presence of the responsible Minister about "privacy, digital data storage and data exchange" (Eerste Kamer 2010-2011).

Nevertheless, most of the projects and proposals related to ICT and information systems appear to have passed through the democratic system virtually unnoticed, even going back many years (see for example Snellen 1992). When an application does attract attention, it is often only after the decision has already been taken. The introduction of the biometric passport and the storage of fingerprints in a central database drew remarkably little public or political attention until the relevant bill had been submitted to the Senate for approval (Böhre 2010; Snijder 2010). Only then did a number of NGOs and scientists stir up something of a public debate. In interviews, some senators admitted that, looking back, they felt they had not kept a close enough eye on the issue.[11] MPs who had previously supported the Government's plans later also expressed concern.

"There are genuine risks [to the storage of biometric data]: fraud, function creep and abuse … It is and will remain a total mystery to me why we Dutch have insisted on taking the lead in this and combining two objectives in a single law, i.e. to combat identity fraud – an objective that I agree with entirely and that I too want to achieve – and to investigate criminal offences, using the database as the binding factor," said Liberal MP Jeanine Hennis-Plasschaert (Tweede Kamer 2010-2011a: 4).

In April 2011, Minister of the Interior and Kingdom Relations Piet-Hein Donner responded to continued criticism by Parliament by putting an end to the central storage of fingerprints and announcing that those fingerprints that had already been stored would be destroyed.[12] Nevertheless, interviews with various MPs show that scrupulous, forward-looking democratic supervision is far from easy, and difficult for many politicians to achieve. That is especially true when plans are developed at the European level, for example relating to Frontex (the EU Border Management Agency) and in the case of the proposed Entry/Exit System at the EU's external borders, according to Senator Pauline Meurs.[13] Members of both the House and the Senate say that their position at the apex of Dutch public administration distances them from many of the systems and applications that they discuss and assess. The debate tends to focus on broad outlines, even though for many technological applications, the devil is in the detail. Some projects also span multiple terms in office, and as the composition of Parliament and coalition governments changes, so do the project objectives. For example, Parliament spent many years discussing the use of biometrics in the passport, and

"… as the years went by, there was a lot of confusion that no one really seemed able to resolve. The terms and aims of biometrics kept expanding: it had to combat everything from 'look-alike fraud' to terrorism, serve as passport verification and identify victims in disasters, and make passports secure as well as prevent identity fraud in general. But the consequences of these high-flown terms for implementation were never identified with any consistency" (Snijder 2010).

Scrupulous parliamentary control is difficult for other reasons as well. For example, Christian Democrat MP Pieter Omtzigt commented that it was not always easy for the House to monitor the progress of a project:

"It's hard to keep close track of major ICT projects. It's also difficult to check up on progress. MPs are naturally given lists of the number of care providers that have joined and other key figures, but the schedules and plans are often much too optimistic" (Pluut 2010: 42).

Omtzigt's observation confirms what the Netherlands Court of Audit previously concluded: government ministers do not inform the House sufficiently, making it very difficult to assess ICT projects before they begin, monitor their progress, and evaluate their effects (Netherlands Court of Audit 2007a).

3.1.6 RESPONSE TO ARGUMENTS

Experience shows that the arguments typically advanced in support of a new information system come in for very little criticism. Although individual public servants and politicians may be sceptical about ICT solutions, partly owing to past fiascos and problems of data contamination, the arguments put forward in the wider debate – security, effectiveness and efficiency – are self-sustaining, especially when combined with the problem-solving 'reputation' of ICT. In everyday politics, they are the 'big guns', often implicitly outweighing other values such as transparency, privacy and, increasingly, freedom of choice. Groothuis (2010), for example, shows that recent amendments to various laws allow government to make the Internet the mandatory channel of communication. Citizens' freedom to choose between paper and digital interaction with government (Tweede Kamer 1997-1998) – a principle firmly rooted in the early days of eGovernment – is gradually being abandoned. At the same time, some government organisations take full advantage of their *own* freedom of choice when transactions on paper are more convenient for them (Groothuis 2010: 351-352).[14] The creation of the anonymous public transport chip card is another sign that freedom of choice rarely takes precedence. The 'anonymous passenger' option was only added to the plans under pressure from the Data Protection Authority (Van 't Hof et al. 2010b), but even after the idea had been accepted, the resulting anonymous chip card turned out to be a less-than-appealing alternative.

In addition, the debate tends to become polarised between politicians and policymakers who prioritise driving principles and those who favour underpinning principles. Upon taking receipt of a report of a special committee on security and privacy (January 2009), the then Minister of the Interior and Kingdom Relations Guusje ter Horst said that it was important to strike a good balance, commenting that a concern for security must not lead to "personal data being thrown up for grabs." Later that same year, however, after the 'underwear bomber' incident in December 2009, her straightforward response was that "security trumps privacy."[15] Polarisation of this kind has been typical of many of the policy-related discussions relating to the utilisation of ICT in recent years. The comments of former Prime Minister Jan Peter Balkenende (then still an MP) during the 2001 meeting between the House and the Minister of the Interior and Kingdom Relations offer a good illustration. The meeting, cited earlier, concerned the need to include a biometric feature in travel documents.

"Mr Balkenende hopes that privacy will not become an impediment to this necessary technical improvement. … Mr Balkenende asks the Minister to confirm that Article 3 of the Passport Act does not concern privacy, but rather [that biometrics concerns] a technical feature that must be incorporated into law" (cited in Böhre 2010: 22).

It is not only security but also the driving principles of effectiveness and efficiency that spur politicians and policymakers on to develop, introduce and use ever newer, more innovative ICT systems. These principles are cited most often as reasons to continue the expansion of eGovernment. The claims made about security, effectiveness and efficiency are, however, often unsubstantiated (Kearns 2004). That is, in any event, the conclusion reached in a study on the digitization of the decision-making process for zoning plans. "Properly substantiated forecasts of the costs and benefits of digitization in the decision-making chain are difficult, if not impossible, to provide" (CapGemini Consulting & Ernst &Young 2004: 8). Various organisations have repeatedly pointed out that the causal relationship assumed between instruments and effects in security policy were not, or not properly, substantiated (Van der Knaap 2010: 13). In its report of May 2009, the Suyver Committee, which evaluated the Netherlands' counter-terrorism policy (Suyver Committee 2009), pointed out the need to evaluate counter-terrorism measures comprehensively. In response, the Government announced an evaluation study whose results are still pending (Tweede Kamer 2008-2009d). The evaluation of ICT has long been a complex issue (Thaens 1998; Van Hout 2005). What is most striking is that the yardstick for evaluating ICT applications is often not the reality of policymaking – or the goals that have been defined – but rather the terms of the system itself, for example how many hits the Reference Index for Juveniles at Risk generates. Real evidence that the application is doing what it was actually intended to do, i.e. improve the social safety net, is almost entirely lacking (compare Waldron 2007; Robinson et al. 2010: 7). The affair of the EPD is a case in point. In a response to the Senate regarding the EPD bill, the Minister of Health commented: "The EPD's added value should … be sought in the ease and speed with which data can be reliably and securely shared" (Eerste Kamer 2009-2010c: 6). According to Pluut (2010), the information provided in the initial policy documents is scarcely more specific than that.

"Policymakers or ministers do not mention studies showing that data-sharing (at national level) has in fact led to these results; nor do they explain how, and under what conditions, a national EPD will lead to improvements in the care sector. They evidently see no reason to do so because in the early years, a sort of general consensus emerged that the Netherlands needed to work toward a nation-wide system of information provision in the care sector" (Pluut 2010: 23).

Only later, as the plans and implementation process proceeded and Parliament grew increasingly critical, did official documents begin to contain more references to research reports demonstrating the need for an EPD. In these arguments, the ultimate aim of the EPD gradually shifted from financial considerations (efficiency) to medical safety.

Box 3.1 Magic with numbers: 19,000 avoidable errors

In their arguments supporting a national EPD, successive ministers have referred to the *HARM Report* (Van den Bemt 2006), based on a study that concludes that of the 41,000 or so medication-related hospital admissions every year, 19,000 are potentially avoidable. The report's most important recommendation is to approach patients who display (or are prone to) one or more risk factors proactively by offering them extra supervision with respect to their medication. The researchers state that better information-sharing is one way to improve such supervision – without, however, explicitly referring to electronic patient dossiers.

In response to questions raised by the opposition during the plenary debate in Parliament on the EPD bill, Minister of Health Ab Klink reiterated: "The data concerning the 19,000 people admitted to hospital and, of these, the 1200 who subsequently died is taken from the HARM study of 2006. What it comes down to is that 60 people are admitted daily owing to errors in their medication, and three of them die every day." MP Arda Gerkens (Socialist Party/SP) responded by asking whether the Minister "had estimated how many medical errors could be avoided by the EPD, or, in other words, how many patients could be expected to improve and what was the chance of the EPD itself leading to errors …"

The Minister replied: "Such an estimate has certainly been made. I had good reason to mention the 19,000 hospital admissions owing to errors in medication. Many of these – but I cannot really say *how* many – could have been avoided if better information had been available on the patient's medication. … I don't think that percentages are so relevant. Even if Accident & Emergency can provide better help in only a few cases a day, then it's already worth it" (Tweede Kamer 2008-2009a: 3936-3937). MP Fleur Agema (Freedom Party/PVV) joined in the debate, stating: "Nowhere in the HARM study does it say that the Electronic Patient Dossier will help reduce the number of avoidable hospital admissions. … My point is that the EPD may reduce the number of avoidable errors – we do not know by how many because Ms Gerkens too was not given an answer to that question – but it may also *increase* the number of avoidable errors. After all, the EPD itself could also contain errors. … The Minister argues that we need the EPD because it will reduce the number of avoidable errors, but – if I may appeal to Klink the scientist – the same reasoning can be applied in the opposite direction. We have no evidence." Minister Klink parried Ms Agema's explanation as follows: "For once, take it on the authority of Klink the scientist that it does work and that it will lead to fewer errors" (Tweede Kamer 2008-2009b: 3946-3947).

The Government has now started to take the targets and indicators for assessing security policy more seriously, following a report by the Netherlands Institute for Social Research (SCP), *Sociale Veiligheid ontsleuteld (*Public Safety Decoded, SCP 2008). Theoretically informed policy reports are gaining ground, but it is only in rare instances that they focus on substantiating expectations and later assessments of ICT initiatives. Some explicitly state that the 'success' of an application cannot be measured, as occurred when questions arose as to whether camera surveillance actually led to greater security.[16] Part of the problem is that no one knows precisely what should be measured or in what units it should be expressed. The Final Report on the Evaluation of Camera Surveillance in Public Places (*Eindrapport Evaluatie cameratoezicht op openbare plaatsen*), published in late 2009, concludes that the effects of camera surveillance on public safety are unclear (Tweede Kamer 2009-2010a).[17] Moreover, while the project costs can be identified, the benefits can not. And even then, the cost projections frequently prove to be too optimistic, with the technology being less durable than anticipated. For example, digitization operations are often budgeted as one-off operations, with no account being taken of long-term expenditure on system maintenance, security, updates, etc. (Keymolen & Prins 2011). The desire to measure the effects of ICT applications sometimes leads to paradoxical consequences. When the UK's House of Commons Home Affairs Committee called on the British Government to investigate whether various security measures, including camera surveillance (CCTV), did in fact lead to a reduction in crime (House of Commons 2008), New Scotland Yard responded by saying that what was first required was a national database of CCTV images.[18]

3.1.7 DRIVING, UNDERPINNING AND PROCESS-BASED PRINCIPLES

How are the driving, underpinning and process-based principles applied in and shaped by political and administrative practice in national government? To begin with, it appears that the interpretation of these principles is far from uniform. This also shows that the task of balancing driving, underpinning and process-based principles is by no means a strictly choreographed affair. Two tendencies appear to influence the erratic way in which these principles are dealt with in the field. The first is the instrumentalist view of ICT. Related to that view is a lack of awareness that ICT can bring about changes in the very nature of government and how it operates.

The above discussion shows that many public administrators who 'own' or advocate ICT applications are inclined to view ICT as an instrument – i.e. a vehicle for policy. They are highly ambitious in what they wish to achieve *with* information technology, but much less ambitious when it comes to setting aims *for* information technology. In the eyes of many policymakers, at least, technology holds out

the promise of doing what they have been doing all along, but better – not differently, merely better. We see this in many different cases, from the way officials tinker with the quality of government service delivery to their attempts to tackle government's duty of care, for example by introducing medication safeguards in the EPD. Among public administrators, the more or less explicit assumption is that the 'primary process' – the actual goals and methods of public policy – will not change. Significantly, this means that they do not, or only barely, acknowledge or perceive the unintended but very real impact that digitization has on the way government operates (the 'primary process'), if only because the public in general has itself changed. Although the instrumental dimension of ICT is important, this attitude has led to a certain paucity of judgment, made clear by the fact that applications are seldom subjected to credible evaluation. There is also a shortage of criteria for assessing applications when the approach taken is purely instrumental. The debate therefore continues to focus on the security of the technology (the public transport chip card) or financial debacles (the various failed ICT projects). In other words, there is a narrow focus on whether the technology has lived up to its promise to do what is already done, but to do it better (more effectively and efficiently). When the discussion is about costs, it is often limited to the staffing or financial implications. The broader implications are not included, and are therefore also not considered in any broader balancing of interests, whether *ex ante* (decision-making) or *ex post* (evaluation). A case in point are the sections of text addressing costs/benefits in the project proposal submitted by the Immigration and Naturalisation Service (IND) as part of the Government programme 'ICT Projects in Social Domains'. The proposal concerned the development of a computerised passport control system (No-Q) for the approximately three million EU passengers who depart from Schiphol each year. The analysis was broken down into the necessary staffing and financial investment on the one hand (costs), and a "quantifiable reduction in lines and waiting times", efficiency improvements when verifying travel documents ('reversing cost increases') and 'security optimisation' on the other (benefits). Both costs and benefits were exclusively subject to an instrumental assessment.[19]

What policymakers also ignore is that ICT can bring about a fundamental change in what are seen as government's responsibilities and duties. According to a close colleague of Neelie Kroes, European Commissioner for Digital Agenda, the idea that information technology is intrinsically meaningless still prevails.[20] But this technology is not – or not only – a *vehicle* of change: it is *itself* a change. Its autonomous significance can even be seen in those areas where digitization has recorded the most value-free progress, specifically in rationalising internal work processes ('operations'). There too, what policymakers hope to achieve *with* ICT is not matched by any aims set *for* ICT. In this context, setting a target *for* ICT would mean genuinely integrating a new application into an organisation so that it becomes intrinsic to its staff and meets their expectations. In practice, the worlds of technol-

ogy and organisation are often kept separate, and eventually it becomes clear that the systems are not really aligned with what is happening on the shop floor (one good example being new ICT system that the police force began using in 2010), and that the intended users are even – for a variety of reasons – undermining or avoiding using the new system. Behind the primary process lies a broad spectrum of work processes and values (Van den Akker & Kuiper 2008: 161). The interaction between the technology and those who work with it changes the way government operates, at times in an unexpected manner. Various examples show that technology can have a powerful influence on government's goals. Current popular policy objectives – for example 'customisation' and proactive policy-making – would be unimaginable without the backdrop of digitization. Nevertheless, ICT is depicted as something neutral, and what is therefore never considered is that such admirable aims as customisation – even when viewed within the context of service delivery – or proactive policymaking cause government itself to change too. That is because such aims assume that government will narrow the gap between itself and the citizen, with everything that implies, be it desirable or undesirable. However, the decisions that lead to these changes are not subject to the sort of broad balancing of interests that also gives full consideration to the underpinning and process-based principles. As we have already seen, for example, opinions in civil society about the EPD are sharply divided – and yet there is no forum that allows all these differing opinions to be expressed at the policymaking level.

3.2 CONCLUSION

ICT has been embraced enthusiastically by politicians and policymakers and has had a clear influence in many different areas of policy. Because there is a strong tendency to think of ICT as an instrument and to colour the debate about digitization in this way, it is much less evident that ICT also fundamentally changes the nature of government, changes how its responsibilities and duties are interpreted, and changes how it operates. There is little or no discussion on these issues and their impact on the relationship between government and citizens – both as individuals and collectively.

With regard to the driving, underpinning and process-based principles, discussions on the consequences of ICT for the driving principles often fall prey to a rhetorical form of accountability (Robinson et al. 2010). There is thought to be little need to argue the case for more effectiveness and more security. As for the consequences for the underpinning principles, what is often lacking is in-depth analysis. In everyday life, these principles are frequently reduced to a section on privacy in the explanatory memorandum accompanying a piece of legislation. Government's very real tendency to make the use of ICT mandatory in the relationship between government and the citizen, and the citizen's diminishing freedom of choice in this matter, are ignored, although it is still, theoretically, the case

that 'unwilling' citizens must be allowed to transact their business through the 'paper channel'. The original proposals for the public transport chip card, for example, did not give passengers the option of travelling anonymously, and the solution devised later was minimalist. There is also little regard for the impact of digitization on the process-based principles or for the need to make appropriate arrangements if something should go wrong. The current Government under Prime Minister Mark Rutte may make it a more explicit priority to bring such principles into balance; the coalition partners (Liberals & Christian Democrats) have agreed that "Information security and personal data protection will be improved. Wherever possible, deadlines will be set for planned measures regarding the storage, linking and processing of personal data and the effectiveness of such measures will be checked thoroughly at the preparatory stage" (official translation of Regeerakkoord VVD-CDA 2010: 56).[21]

It will only be possible to take the more comprehensive approach intrinsic to realistically balancing driving, underpinning and process-based principles when ICT has become politicised. As will be clear from the discussion above, that is in fact gradually happening, thanks to the efforts of the Senate, the House, and organised groups of citizens. The situation is still volatile, however; it is difficult to predict which topics (applications) will and will not attract attention. It is clear in any event that, where a proposed application obviously represents interference in social relations, it will be introduced by means of the most rigorous instrument possible, i.e. an Act of Parliament. But even then, debate can be neutralised by exaggerated trust in ICT (as an instrument), as occurred initially in the case of the biometric database. When the proposed application resembles a neutral technical 'gadget', the tendency will be to avoid any discussion of the topic. But vital social issues can be found even in 'gadget-like' subjects such as the BSN. The point is to survey the wider consequences as comprehensively as possible and weigh up the pros and cons.

The most important conclusion, however, is that, despite a tendency to view technology and applications from an instrumentalist perspective, fierce debates sometimes arise about them – but that such debates are virtually nonexistent when it comes to information flows and links between applications. The many examples given above show that there have been few if any attempts to assign autonomous significance to information flows and links or to acknowledge such significance politically. Accountability with respect to these issues is often even less evident than in the case of applications. The most elaborate justification that can be found is something along the lines of "We will link files X and Y because doing so will produce potential advantage Z." Even in such cases, the question is narrowed down to the desirability of the target (Z). The only attempt at evaluation is to ask whether ICT has made it easier to achieve that target. Accountability for information flows, it seems, has not become part of the mental framework of politicians and policymakers.

NOTES

1 For more details, see Böhre 2010.

2 See, for example, the No-Q pilot launched at Schiphol Airport on 26 May 2010: http://english.justitie.nl/currenttopics/pressreleases/archives-2010/100525electronic-border-crossing-starts-today.aspx?cp=35&cs=1578.

3 NUP (2008) National Implementation Programme on Service Delivery and eGovernment. 'Citizen and Business at the Centre', accompanying the statement dated 1 December 2008, adopted at the Administrative Consultations of national, provincial and local authorities and water boards relating to the National Implementation Programme on Service Delivery and eGovernment, p. 3.

4 For an overview, see House of Representatives 2009-2010k.

5 CIOT stands for *Centraal Informatiepunt Onderzoek Telecommunicatie* (Central Information Point for Telecommunication Investigation).

6 Interview with Mr Maarten Hillenaar, Coordinating CIO, November 2009, March 2010, Ministry of the Interior and Kingdom Relations.

7 *NRC Handelsblad* 'En opnieuw haalt het EPD het niet: operatie mislukt, minister gered', 30 March 2011.

8 These are the so called PNR-data.

9 The Centre of Expertise, letter relating to assessment of cost-benefit analysis of No-Q, The Hague, 15 December 2008.

10 Highly critical of this proposal: Raad van State 2010: 141-142.

11 Interview with Senators R.H. van de Beeten, H. Franken, J. Hamel, P.L. Meurs, I.Y. Tan, C.P. Thissen; May 2010. Members and policy advisors of the Council of State expressed similar sentiments, April 2010 (interview with C.J.M. Schuyt, M. Oosting, M. Raijmakers, H.J.T.M. van Roosmalen, and Council of State). The Council had issued an *advies-conform* (advice consisting of an unreserved endorsemenet) during the passage through Parliament of the bill relating to biometrics in passports.

12 *Algemeen Dagblad* 'Veel gejuich om besluit vingerafdrukken niet op te slaan', 28 april 2011

13 Interview with Senators R.H. van de Beeten, H. Franken, J. Hamel, P.L. Meurs, I.Y. Tan, C.P. Thissen; May 2010.

14 For example, the case law relating to Article 2:15 of the Administrative Law Act (AWB) provides various examples of situations in which a government organisation found it inconvenient (later) to communicate through a digital channel and the organisation then took the formal view that the digital channel was not available (Groothuis 2010).

15 Guusje Ter Horst made this statement on 30 December 2009 during a press conference on the abortive attack on a flight from Amsterdam Schiphol to Detroit five days earlier.

16 The commercial research firm Regioplan has developed a Decision-making Tool for Continuing Camera Surveillance (BICC), giving local authorities a basis for evaluation and for taking an informed decision as to whether to cease or continue camera surveillance. *Secondant* 3-4 2010: 58-61.

17 The same conclusion was reached in the United Kingdom, in a study carried out by the Liberal Democrats: www.thisislondon.co.uk/news/article-23412867-tens-of-thousands-of-cctv-cameras-yet-80-of-crime-unsolved.do.

18 www.guardian.co.uk/uk/2008/may/06/ukcrime1.

19 Immigration and Naturalisation Service (IND), Aanvraag investeringsimpuls ICT in maatschappelijk domein (Application for Investment Incentive ICT in the Community), No-Q project plan, 15 December 2008.

20 Interview with Constantijn van Oranje, office of European Commissioner Neelie Kroes, Brussels, March 2010.

21 www.government.nl/dsc?c=getobject&s=obj&objectid=127729.

4 FROM POLICY TO REALITY

It is not only politicians and policymakers in The Hague who have set ambitious targets for new systems and who are calling for more and better information. In addition to the national plans debated in the Senate and House of Representatives, a variety of local authorities and government agencies are working on their own plans and projects, relatively independently and far removed from parliamentary control. eGovernment is not only being rolled out 'on the shop floor'; it is also being built there to a significant degree. There is ample scope for bottom-up initiatives. The national systems debated in Parliament are often nothing more than a platform for a multitude of existing local initiatives. That is the case, for example, with the EPD and the Reference Index for Juveniles at Risk. Prior to the official launch of a system – either by national government, a government agency, or a local authority – it has often been trialled extensively in the field, for example in a certified pilot project or in everyday practice, regardless of any formal decision-making. One example of the latter is the practice of Automatic Number Plate Recognition (ANPR, see Section 4.3). There is therefore every reason to examine the user side of eGovernment applications, particularly when the user and the developer are one and the same. That is the case for the Tax and Customs Administration and other large-scale administrative agencies that have long led the way in promoting the benefits of digitization. Local government officials have also been active in that respect, with local needs and requirements inspiring local authorities to develop their own, more tailor-made approach to the electronic child dossier, for example. The police are gradually extending their information toolkit; the Work and Income Chain Computerisation Office (*Bureau Keteninformatisering Werk en Inkomen*, BKWI) has grown into a crucial source of data for all the organisations acting under the Organisation of Employment and Income Act (*Wet Structuur Uitvoeringsorganisatie Werk en Inkomen*, SUWI), which in turn cooperate with one another on the digital client dossier (*digitaal klantdossier*, DKD). The Tax and Customs Administration allows taxpayers to submit their returns online through a secure portal, and the Social Insurance Bank (SVB) is working to extend the 'Citizen Policy' website (www.burgerpolis.nl), where individuals can request a personalised statement of their social security status and share stories about their experience of the social security system.

4.1 IMPLEMENTATION WITHOUT BOUNDARIES

4.1.1 SO MANY ACTORS, SO MANY REASONS

The Centre for Vehicle Technology and Information (*Rijksdienst voor het Wegverkeer*, RDW) has been hard at work in recent years making a business case for the electronic driving licence ('eLicence'). "In conclusion, it will be possible to place a

chip on the driving licence, something that can help combat fraud and provide a valuable electronic service" (RDW 2008: 5). The RDW wants to use the driving licence chip, an option provided for under the third EU Directive on driving licences,[1] for something more than simply meeting the EU's new anti-fraud requirements. It has recognised an opportunity to play a key role in eGovernment by turning the driving licence into a generally applicable form of ID that offers electronic authentication with a high degree of security[2] for all kinds of digital government services. The RDW can be ambitious in this respect largely because government has not yet come up with an authentication tool providing security at such a high level. Right now, it is only private actors that offer such a tool, and the public infrastructure provided by the DigiD system (which works with a password and text-message system) will be made inadequate by such plans as those offering patients the option of reviewing – or even amending – the data in their EPD, or allowing individuals to overwrite their number plate registration number electronically. At least three ministries have spied an opportunity to position themselves as future leaders in eGovernment and have launched their own authentication initiatives. In addition to the RDW's eLicence, the Ministry of Economic Affairs has also stepped into the ring with its eRecognition programme, while the Ministry of the Interior and Kingdom Relations is introducing a new version of DigiD and a follow-up to the earlier, unsuccessful, electronic Identity Card (eNIK). What these initiatives have in common is that most of the relevant stakeholders consider the involvement of commercial partners crucial to the system's success (CapGemini Consulting 2010a: 14). Public-private partnership appears to be the prevailing motto: "The RDW is considering making electronic authentication available to private parties as well" (RDW 2008: 15).

There are many reasons why organisations may wish to transcend their own boundaries at the operational level and share applications (for example an ID card) and information with others. For the RDW, the reasons lie not only in the need to combat fraud and streamline services; they are also related to its position in the eGovernment of tomorrow. Some partnerships are created out of the 'pure necessity' of tackling complex social problems jointly, according to the initiators. Programmes meant to improve aspects of public safety, such as the Reference Index for Juveniles at Risk, are a case in point (Keymolen & Prins 2011; Holvast & Bonthuis 2010). Other partnerships are established because it would be impossible to undertake complex policy initiatives involving multiple organisations (benefits, care allowances) in any other way and have them succeed. Sometimes the decision to join forces is made very explicitly, for instance in the case of the Manifesto Group, set up by eleven such agencies[3] to supply the public and businesses with government-wide information and services. More generally, bottom-up initiatives often spring from inadequate eGovernment policy at ministry level (Gateway NUP 2009).[4]

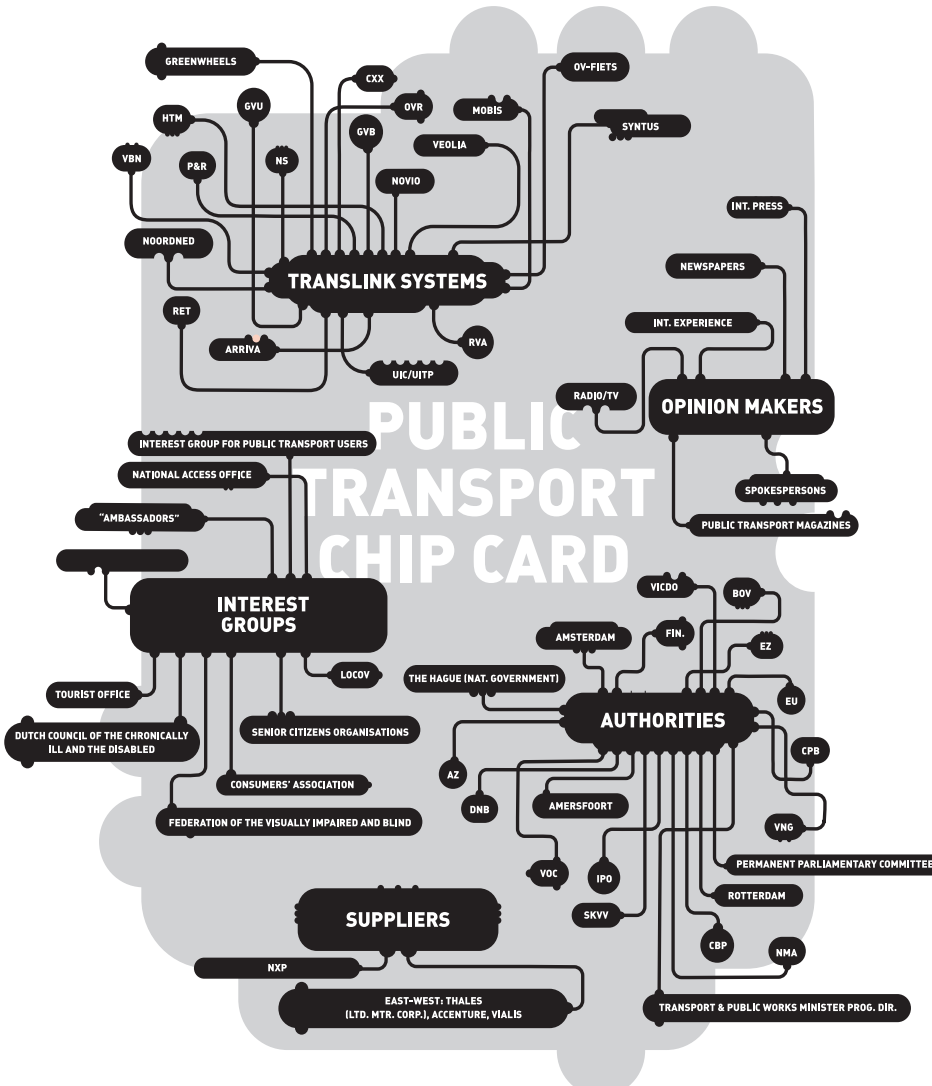
In short, ICT is used in a wide variety of ways in the everyday work of government: projects are launched for all kinds of reasons, partnerships take many different forms, the information-sharing mechanisms vary widely, and the stakeholders are extremely diverse. If a single, unified eGovernment exists at all, it is not at the operational level. What is more, many of the organisations working at this level lack a well-defined structure or coherent staffing and budgeting system. "One of the hallmarks of a virtual organisation is precisely the lack of a clearly defined structure and distinct organisational boundaries. Virtual organisations are often organisations in transition, with ever-changing processes of electronic inclusion and exclusion" (Bekkers 2000: 12). One obvious case is the RINIS Foundation (Institute for the Routing of (Inter)National Information Streams), which serves as a broker between information supply and demand. Originally, it was the Social Insurance Bank (SVB), the National Social Insurance Collection Agency (*Landelijk Bureau Inning Sociale Verzekeringen*) and the National Social Insurance Institute (*Landelijk Instituut Sociale Verzekeringen*) that took the first step toward multisector data-sharing by setting up RINIS (Kinkhorst 2000: 182; Bekkers & Thaens 2005: 143). RINIS now offers services to 11 'sectors'[5] and in 2009 handled more than 177 million messages (RINIS 2010: 3), almost double the number in 2008. Data is also exchanged with organisations abroad: SVB and the Health Care Insurance Board (*College voor Zorgverzekeringen*, CVZ) use RINIS to exchange messages with their European sister organisations (RINIS 2010). Bekkers refers in this connection to 'colonisation' and the 'blurring of boundaries': "RINIS is integrating a growing list of domains that lie outside the field of social insurance. It continues to extend its territory, and that means that the boundaries between all sorts of policy domains are beginning to erode" (Bekkers 1998: 139-140).

4.1.2 OVERLAPPING POLICY DOMAINS, SERVICES AND MOTIVES

It was more than a decade ago that Bekkers recognised the first signs of boundary erosion due to ICT. Today, dismantlement is in full swing. In many cases, one and the same application or source of information is used for service, care and control, and different applications increasingly make use of the same data. There are numerous examples, and a glance at the list of notifications maintained by the Data Protection Authority reveals many strange bedfellows. As 'partners in the chain' (in reality, as network partners), organisations such as the Social Security Agency (UWV), the Centre for Work and Income (CWI), and the Social Insurance Bank (SVB) have long shared employment and income data with the help of the Work and Income Chain Computerisation Office (BKWI). A few years ago, however, the Labour Inspectorate (*Arbeidsinspectie*), the Social Intelligence and Investigation Service (*Sociale Inlichtingen en Opsporingsdienst*, SIOD) and other similar investigation agencies also joined in. In 2010, the Data Protection Authority investigated SIOD's practice of drawing up risk profiles based on data obtained from municipal officials, the Tax and Customs Administration, and the Public

Prosecutions Service, which it used not only to investigate benefit fraud but also to track individuals suspected of carrying a risk of criminal or anti-social behaviour, or who might benefit from extra support. In the latter case, SIOD also used data provided by school attendance officers to create links and generate profiles (CBP 2010b).

Figure 4.1 **Input for the development of the Public Transport Chip Card**



Based on the OV2Pay program, in ECP-EPN (2010: 23)

Another example relates to data-sharing by the Education Executive Agency (*Dienst Uitvoering Onderwijs*, DUO). DUO shares data – not always anonymised – with the Municipal Personal Records Database, Municipal Social Services, the Tax and Customs Administration, the Social Insurance Bank, the Ministry of Justice, various educational institutions, and certified school and career consultants. "In addition, it is possible that the Minister of Education, Culture and Science will hire Statistics Netherlands (CBS) or a commercial research firm to approach a specific client group."[6]

The situation was equally complex in the case of the public transport chip card, which involved a convoluted combination of services, actors and sectors. As figure 4.1 shows, dozens of parties signed up while the initial plans were still on the drawing board: various public authorities (the Ministry of Transport, Public Works and Water Management and 35 government authorities active in the area of public transport), a wide range of transport companies, passenger organisations, the Royal Dutch Touring Club (ANWB), and a whole range of third parties, including 'card issuers' (banks, a supermarket chain) and the suppliers of the communication systems and other equipment (De Kok et al. 2001; 298).

The Tax and Customs Administration has turned itself into a key exchange for fraud investigations in the social security and care sectors. Various members of the Senate have commented in interviews that data is linked selectively, however; links are created to track down fraud, but not to trace individuals entitled to allowances.[7] The Tax and Customs Administration has long been authorised to request information from third parties (Zwenne 1998), but it now gathers increasingly large quantities of information behind the backs of taxpayers in order to "avoid increasing the amount of red tape that the citizen is obliged to deal with."[8] It not only gathers information from familiar sources such as the Land Registry, Chambers of Commerce, employers or banks, but also from websites such as eBay, LinkedIn and social networking media.

Cooperation is also no longer just a question of individuals deciding to share data and dossiers; domains sometimes overlap via entirely automated processes. For example, when the Central Fine Collection Agency (*Centraal Justitieel Incasso Bureau*, CJIB) decides to collect an unpaid traffic fine, it is, officially at least, the public prosecutor who takes the decision. In practice, however, the procedure is entirely automatic and it is a computer that issues the collection order. The CJIB can then "use RINIS's computerised reference index to recover fines from income derived from employment and recurrent benefits without a writ of execution having to be issued" (Bekkers 1998: 93). Service and control are opposite sides of the same coin, according to Steven Luitjens and Dirk Schravendeel, two of the people who led the introduction of the 'basic records database'.

"Basic records databases make data transfers possible. Government can take advantage of this option to check up on citizens and keep control of them, but it can also use it to provide a better service to citizens . . ., to involve them more in the democratic process and to clarify what data government has and what it does with that data. [These are] opposite sides of the same coin" (Schravendeel and Luitjens 2001: 362).

4.1.3 THE eOPERATIONS TOOLKIT

In terms of operational procedures, of course, the practice of merging information processes and making the boundaries between policy domains fluid is not entirely new. Various administrative agencies have long made it possible for other partners in the public sector to consult their systems online and even alter data in them (Bekkers 1998: 135). As far back as the 1990s, researchers grew interested in the influence of computers on the relationship between policymaking and policy implementation and on the traditional boundaries between policy sectors at the operational level (Snellen 1994; Van de Donk & Frissen 1994). Authors even came up with sleek new names for this 'new' government: 'linked-up state' (Hirsch Ballin 1993), 'virtual fortress' (Taylor & Van Every 1993), 'infocracy' (Zuurmond 1994) and 'virtual state' (Frissen 1996). Since then, the job of building this 'other' government has been tackled with mounting enthusiasm. Recent policy initiatives – the streamlining of basic records, the reference indexes, and the popularity of working in 'chains' (in fact, often networks) – have increased the speed at which operational procedures have been digitally interlinked in recent years. The new toolkit is also gradually changing government's administrative reality, and that reality appears, in turn, to be increasingly shaping the way government views society. The most important types of arrangement are:

- Working in regulatory chains and networks;
- Multiple applications, organisations and e-dossiers making use of the same data;
- Creating reference indexes,[9] interfaces[10] and national exchanges[11] for the necessary connections and the resulting the data flows within the chains and between the dossiers;
- Streamlining this data traffic using the Citizen Service Number (BSN) and authentic records so that every organisation has access to a single, unique personal ID number and an authoritative source of information.

"In theory, then, it should always be clear where the information can be found and who is responsible for it. It should also (theoretically) be clear what purpose the information serves and that the information that is found can be trusted" (Netherlands Court of Audit 2010a: 18). Things are somewhat less reliable in practice, however – as Ron Kowsoleea and other victims of identity theft can attest (Buruma 2011; Office of the National Ombudsman 2009a). Another clear indicator is the attitude of the Tax and Customs Administration toward the use of the Municipal Personal

Records Database (GBA). Because the quality of the GBA is not entirely guaranteed, the Tax and Customs Administration has insisted that the Ministry of the Interior and Kingdom Relations allow it to deviate from the basic records database. If a taxpayer says that his or her GBA record is incorrect, Tax and Customs bases its assessment on the data that the taxpayer supplies (Tweede Kamer 2009-2010i). Minister of Finance Jan Kees de Jager had this to say at a meeting with the parliamentary finance committee: "The idea behind the GBA is a very good one, but it's clear that one part of the supply chain that Tax and Customs cannot control nevertheless has an indirect impact on the services it provides" (Tweede Kamer 2010-2011b: 11-12).

What are typical targets for the various tools in the eGovernment toolkit? An ICT-based supply chain or network approach aims to dismantle the partitions between different organisations, making them more efficient and allowing them to work in a more problem-based or demand-driven fashion (SUWI Expert Committee on Information Provision and Electronic Service Delivery 2005; Van Duivenboden et al. 2000; Grijpink 2006a). Digital dossiers facilitate data-sharing, for example data on indicators shared between the Social Security Agency (UWV), the UWV Job Centre (*UWV-werkbedrijf*), the Care Needs Assessment Centre (CIZ), MEE[12] and local government within the context of various unemployment and social benefits programmes (WMO, AWBZ, WAJONG, WSW and WIA).[13] Interfaces, reference indexes and national exchanges are instrumental in joining up a patchwork of tens of thousands of local databases and as many electronic dossiers housed in countless public and semi-public organisations. The EPD is one such national exchange. It would have allowed – had it not been rejected by the Senate – authorised individuals to request information that is held by various care providers (Pluut 2010). It is therefore not a centrally stored digital dossier, but an infrastructure that allows for information sharing. The EPD and other infrastructures make use of the BSN, a unique, general and non-informational personal number that identifies individuals in their transactions with government (Tweede Kamer 2005-2006a). It is also a serial number that helps prevent duplication of data files within government and unlocks the system of basic data and authentic records. "Although it is not yet a policy priority to use the BSN in police and other investigations, there is little doubt that that will quickly change," commented a consultancy firm some years ago (HEC 2007: 70). Authentic records and basic data can also guarantee all kinds of partnerships and supply chains within government a single, unequivocal, authoritative source of information (Tweede Kamer 2000-2001b). The main idea behind the basic records databases is that local authorities and government agencies need only ask citizens and businesses for information once, and that use of that information is then compulsory within government. Basic records are considered the key to alleviating the administrative burden, delivering public services, combating fraud, streamlining the internal machinery of government, and making policy data available. They are now referred to as the *system of basic records databases*,[14] indicating that the legal, informational, technical and organisational coor-

dination and links between records are such that they can be used throughout government. In that sense, they are the 'backbone' of government information management.[15] Basic records databases contain legally binding facts about a growing number of 'objects' subject to government jurisdiction (people, cars, buildings, streets, etc.). These facts, which constitute the basic data for a rising number of government applications, are consequently being used by a growing number of public-sector organisations. In theory, the system of basic records databases offers an excellent opportunity to strengthen the position of the citizen, for example because it could be designed in a way that makes it easier for people to alter the data, submit applications or requests, or claim certain rights. So far, however, government has not made much use of the emancipatory potential of the basic records databases (Boschker, Castenmiller & Zuurmond 2010: 97-98).

All in all, the eOperations toolkit consists of a burgeoning collection of technical facilities that includes databases and standardised information such as unique numbers. Standardisation, normalisation and the semantic interoperability[16] of all these facilities are considered crucial issues (Standardisation Board & Forum 2009). In order to ensure that every tool in the toolkit works seamlessly with the others, the relevant targets, constituent parts and agreements have been set out in the National Implementation Programme for Service Delivery and eGovernment (*Nationaal Uitvoerings Programma Dienstverlening en eOverheid*, NUP) and in the Dutch Government Reference Architecture (*Nederlandse Overheids Referentie Architectuur*, NORA); regarding interoperability, the Office of the Standardisation Forum (*Bureau Forum Standaardisatie*) – consisting of experts from government and the business world – plays a coordinating and facilitating role (Forum Standaardisatie 2010). The Forum acts as a think tank for the Standardisation Board (*College Standaardisatie*), whose members are senior civil servants. It is proving to be quite a challenge to develop some of the tools in the toolkit, as evidenced by the devastating gateway review of the NUP that a special review committee (chaired by Arthur Docters van Leeuwen[17]) sent to the House of Representatives early in 2010 (Gateway NUP 2009).

4.1.4 A CHANGING ADMINISTRATIVE REALITY

Government information management is changing, step by step and in fits and starts. And it is precisely at the 'street' or operational level – where organisations work most closely with citizens and communicate regularly with them – that we see most clearly how the new information management is changing government's relationship with the citizen and the position of citizens. In the late 1980s, Frissen predicted that databases would become "the 'Archimedean point' from which social collectivities would be planned" (Frissen 1989: 260). Ten years later, Van Duivenboden examined data-linking practices at the Municipal Social Services and the RDW and concluded that in both cases, these practices were shifting the

burden of proof from government to the citizen (Van Duivenboden 1999: 322). For example, the linking up of databases at the RDW had shifted the burden of proof "to the vehicle owner, who will himself have to approach the GBA, the Tax and Customs Administration or his insurance company. . . . In that sense, there is a relationship between building and expanding a virtual records database and increasing the citizen's responsibility for setting an erroneous record straight" (Van Duivenboden 1999: 229). This trend has been confirmed in reports by the Office of the National Ombudsman stating that the RDW has compared vehicle registration records, insurance records, and the motor vehicle test records "from the current all the way back to January 1995" (Office of the National Ombudsman 2008; Office of the National Ombudsman 2009b). A decade later, Overkleeft-Verburg found in her examination of case law that judges are indeed increasingly inclined to hold citizens accountable when incorrect data is used (Overkleeft-Verburg 2009: 74). The same trend can be seen in the United States, with responsibilities previously borne by government and businesses being progressively shifted to the individual citizen, in this case with respect to identity fraud (Whitson & Haggerty 2008). But there are also other changes afoot. Specifically, new information management systems also divide processes and responsibilities between different government bodies: the introduction of basic records databases means that the responsibility for taking the final decision, for example on an application or a request for a benefit, is now separate from the responsibility for keeping the basic records straight on which that decision is based. What that means for citizens is that they must now deal with two government bodies instead of one, as in the past.

In addition to the shift in their respective positions, the public authorities and citizens also find themselves becoming vulnerable in new ways. For government, the new vulnerabilities include increasing system abuse (Govcert.nl 2009: 9), deficient digital archiving, and the inability to view data in its historical or other context or to prioritise data according to importance, vulnerability or sensitivity, or to check its accuracy. A case in point is a report by the Office of the National Ombudsman on a procedure used by the Tax and Customs Administatration to monitor people setting up a business. The procedure involves comparing files maintained by the Tax and Customs Administration (tax rebate for self-employed people) and by the Social Security Agency (reported number of hours worked). Based on this comparison, the level of fraud in the relevant years (2007, 2008 and 2009) was taken to be between 26 per cent and 40 per cent. Almost 3000 self-employed people subsequently received demands for payment of back taxes, had sanctions imposed on them, or were even liable to prosecution. When the Office of the National Ombudsman investigated the matter, it found that the two files had been compared without any consideration being given to the meaning of the data in its individual context. Many of those accused of fraud ultimately turned out to be innocent of any wrongdoing (Office of the National Ombudsman 2010b).

For the public, many of the new vulnerabilities are related to the networked nature of information – in other words, the shared use and management of information in a network of actors that arises through the supply chains, interfaces, reference indexes, etc. mentioned earlier. Such 'networking' is often regarded as nothing more than a technical exercise, but in reality its repercussions go much further. As noted earlier, the supply-chain approach has led to a growing number of organisations becoming interwoven through their systems, with the Citizen Service Number (BSN) playing a crucial role. Technology facilities the interconnections and makes information flows between organisations possible, but the corresponding connections in terms of responsibilities and liabilities are frequently not forthcoming. In short, the legal semantics cannot keep pace with the technical semantics. The same observation was made in a recent government 'trend report' (a biennial publication) on trends in local public administration: there is a much greater level of cooperation than there used to be, but the common denominator in all the partnerships is that the partners retain their autonomy in policymaking (Ministerie van BZK 2010: 36). That means that responsibility is still defined institutionally, along the lines of the traditional structures of public administration.

The result is that responsibility for information processes is fragmented (with different actors responsible for different segments of the chain), or that it more or less 'disappears', because the various parties are able to do nothing more than refer cases to one another if the transition to ICT has simply not been interpreted in terms of responsibilities. In short, the use of technology and the idea of organising policy-related information about citizens into chains conflicts with the traditional hierarchy of government. In both a technical and in a practical sense, people in fact already work within chains (or networks), but the decision-making, the division of responsibilities, the legislation and the supervision mechanisms have not yet been tailored to reflect these new practices. What is lacking is an overall strategy for organising coordination and responsibility when information is circulated in networks and chains of government organisations (Borst 2009: 262). What is also missing, according to various insiders, is an organisation that takes binding decisions when problems such as identity fraud arise, or when no one organisation is prepared to 'own' a problem and take responsibility for errors in the chain. For example, in a study of the problems that the BSN has caused citizens, a consultancy firm reports:

> "As far as we are aware, the Ministers involved in implementation schemes that make use of the BSN have not made any specific policy arrangements concerning vigilance in this regard, or appointed an official who has the authority to review such cases and assist the relevant citizen. We do not believe that the Data Protection Official provided for in the Citizen Service Number (General Provisions) Act has either the necessary position or the requisite powers" (HEC 2007: 68).

4.1.5 BEYOND EFFECTIVENESS AND EFFICIENCY

Ultimately, government's stated aims and the new tools available should contribute to improving service delivery, care and control. Even at the operational level, however, it is difficult to decide how to measure that contribution and what criteria should be applied. Should effectiveness and efficiency be the yardstick, or a much broader set of criteria, such as those defined in the 'Citizen Service Code'?[18] The State Secretary for the Interior said the following about the Code in 2007: "It is only one of the instruments available to us. I have yet to decide whether and how we will use it" (Burger@Overheid.nl 2007: 94). The new technologies can vastly improve efficiency, and in the best-case scenario, one could say that what is efficient for government is also efficient for the citizen. Johan Hakkenberg, director of the RDW and chairman of the Manifesto Group, pointed out the advantages for both the public and government of the 'Message Box', a "secure e-mail system that enables users to exchange digital messages with Dutch government agencies at national, provincial and municipal level, as well as with the water boards" (see www.answersforbusiness.nl/messagebox).[19] Citizens are free to decide to receive communications from the relevant agencies in their Message Box, rather than on paper. The Message Box offers them a facility for receiving information and for transacting business with government, but it also serves as an archive. Each year, government agencies send out 600 million letters. Cutting the number sent by post by 100 million not only creates a new public service but also represents a significant cost reduction. Another opportunity that has been taken advantage of relates to the RDW website. After consulting a user group, the RDW decided to organise the site by target group and from the client's perspective. It now gets 30 million hits a year. Online transactions through the site's self-service facility are particularly popular; they save clients money and are available 24/7. For example, now that it is possible to suspend a vehicle registration online, the number of suspensions has increased by 40 to 50 per cent. According to Hakkenberg, an enormous number of visitors also wish to inspect their own personal data. Finally, the following passage, taken from the 2008 Annual Report of the IB Group – the government agency that administers student grants and loans, now part of DUO – can serve as an example:

> "In 2008, clients logged in to My IB-Group 2.9 million times to inspect their personal data. In more than 600,000 cases, visitors amended that data digitally. In addition, 2008 was the first year that students were able to indicate on My IB-Group whether they wanted to receive digital notifications about their student grant or loan. Some 375,000 notifications were sent digitally rather than by regular post. 2008 was also the first year that proactive e-mails containing customised information were sent to My IB-Group users. For example, the IB-Group sent an e-mail alert to prospective students who had already enrolled in a higher education programme but had not yet requested a student grant" (IB-Group 2009: 20).

In addition to driving principles, however, underpinning principles such as privacy are also given their due at the operational level. Although privacy is not considered important in every context (Zenc 2007: 77), and although both the CPB and the Office of the National Ombudsman have regularly publicised cases in which government agencies have violated an individual's privacy, it is certainly a principle etched into the consciousness of the larger agencies, in any event. A study conducted by Van Duivenboden more than a decade ago already revealed a concern for privacy at the Municipal Social Services and the RDW (Van Duivenboden 1999: 234). When agencies are particularly keen to respect their clients' privacy, this is in part because they work very closely with the public and communicate regularly with citizens. In some cases, privacy is also an explicit factor in the 'business case' for a new e-service, precisely because the success of the initiative depends on its being accepted by the public. Van Duivenboden's study demonstrated a relationship between an organisation's struggle to maintain autonomy on the one hand and scrupulousness when dealing with personal data on the other: "In addition, making explicit agreements as to which data may be inspected or received and vice versa also supports the Municipal Social Services' desire to operate as autonomously as possible" (Van Duivenboden 1999: 178). This observation is important, given that the desire to work in networks and chains and through exchanges appears to be detrimental to privacy. Many of the individuals interviewed for this book have observed that networks and chains are linked at the interface between the public and private sectors, but that there is no adequate regulatory arrangement to monitor the way the private sector uses the data it obtains from the public sector. Henk Tankink and Jan Willem van Dongen of the Personal Records Database and Travel Documents Agency (BPR Agency) comment as follows:

"The GBA supplies information to pension insurers, motor vehicle inspectors, bailiffs and other parties as part of their public tasks. But these parties work in the private as well as in the public sector. Although the procedure that leads up to the supply of data is quite strict thanks to the log-in system, once the data has been provided, monitoring is limited and there is no supervision of how it will ultimately be used."[20]

With so many different partners in the chain, a host of practical problems have arisen relating to the quality of that data and whether it is being dealt with scrupulously enough. The Office of the National Ombudsman concludes: "Chain computerisation can perhaps solve certain administrative problems and quicken the pace of innovation in government, but there is little reason to rely too much on its effects" (Office of the National Ombudsman 2009a: 28).

The process-based principles of transparency and accountability appear to be under pressure at the operational level, however. We referred previously to the

fragmentation of responsibility, and even to its occasional 'disappearance' in cooperating networks and chains. One good example is the case mentioned earlier of the social services inspectors, who link up a large number of files in order to generate risk profiles. The Data Protection Authority told the Social Intelligence and Investigation Service (SIOD) that it should have informed the individuals in question; SIOD responded by saying that it considered that the job of the regional intervention teams. After all, argued SIOD, it was they who supplied the indicators showing a higher risk of benefits fraud (CBP 2010b). Transparency – for purposes of democratic engagement and supervision – has also turned out to be difficult. Straten (1996: 254) concludes that politics had been sidelined while the GBA was being developed. Based on studies relating to the IB Group (student grants and loans) and the Central Fine Collection Agency (CJIB), Zouridis (2000: 318) claims that the process of developing ICT systems within these organisations had proved so unwieldy and complex that political involvement had been minimal. "Does the law play the coordinating and regulatory role that we assume it does, given the primacy of the legislator and of political deliberations? Or are we rather witnessing that the law itself is becoming the product of interactions with the organisation and ICT?" (Zouridis 2000: 318). The answer to these questions is all the more urgent given Zouridis's observation that there are gaps in the way accountability for systems development is organised: "For example, how transparent is the algorithm in the computer system? In the case of student financial aid, the system has been referred to as 'full of spots and blemishes' and difficult even for insiders to comprehend …" (Zouridis 2000: 315). The case of the Reference Index for Juveniles at Risk shows, moreover, that the statutory foundations are often provided only after the projects have been up and running for quite some time and their structure and design have long been decided (what data is to be included, who is to supply the data, who will have access to it, what other initiatives will be linked to it, etc.) (Keymolen & Prins 2011).

4.2 LOCAL STRUGGLES

On 28 October 2009, the Board of Chief Commissioners adopted their strategic agenda on camera surveillance, entitled *Beelden van de Samenleving* (Images of Society). The foreword outlines the problems and dilemmas that the police face.

> "Public and private camera surveillance has so far been insufficiently professional and coherent. In addition, public and private parties are increasingly making use of intelligent camera systems, which compare observations and recorded images of persons and vehicles with a variety of different databases. The question that we are faced with is: what are the limits? There is risk involved in pursuing data because it is conducive to public safety and security, and in exploiting the advantages of technology: the risk of gathering and interlinking vast quantities of – often unnecessary – information. This is undesirable from the vantage point of privacy" (Board of Chief Commissioners 2009: 3).

Local authorities and the police play a key role in how ICT is used at local and regional level. What is typical of the dynamics at this level is that both parties act with relative autonomy, resulting in an extremely wide range of initiatives, practices and criteria. Also typical, however, is that both struggle palpably with a dilemma: on the one hand, they are keen to take advantage of the unparalleled advantages of digitization for their work; on the other, they themselves believe there should be limits to what they are permitted to do. Many of the local administrators and officials interviewed for this book said they were dissatisfied and frustrated by the lack of guidance at the national level when faced with decisions. They felt they had been abandoned by a whole host of organisations and institutions, ranging from the Association of Dutch Municipalities (*Vereniging Nederlandse Gemeenten*, VNG) and the Data Protection Authority to the ministries responsible. The committee that conducted the gateway review of the NUP (mentioned earlier) makes the same point:

> "Many respondents are specifically critical of VNG's failure to play a proactive role thus far and its reluctance to take the lead on topics that require concerted action and standardisation. The same criticism was also levelled at the Ministry of the Interior as the 'coordinating ministry'" (Gateway NUP 2009).

4.2.1 LOCAL AUTHORITIES 2.0

Local authorities have their own reasons for undertaking ICT innovation (for example digital tracking systems for permit requests, new back-office data warehousing concepts), but above all else, they play a key role in helping national government achieve its various digitization aims. These aims initially concerned digital service delivery, with projects ranging from e-forms, personalised web functions on *MijnOverheid.nl* (MyGovernment.nl), and linking municipal services to the DigiD system to revamping the GBA, simultaneously introducing authentic records and basic personal data, and, recently, launching the *Antwoord*© initiative (Answer©), which makes the local authority (i.e. the *digital* local authority) the key resource for citizens' FAQs.[21]

More recently, however, local authorities have also played an important role in rolling out ICT initiatives related to control (issuing passports and, as a result, applying biometrics) and care and control (Reference Index for Juveniles at Risk and the 'Safe Houses' described above). It is clear that the boundaries are shifting at the local level as well, especially the boundaries between differing policy domains. Care is being linked to control, as in the Reference Index for Juveniles at Risk. But the boundaries between the public, semi-public and private sectors are also becoming blurred. The organisations participating in the National Debt Information System (*Landelijk Informatiesysteem Schulden*, LIS) include not only local

authorities (municipal social services department), but also energy companies, housing corporations, members of the Association for Debt Assistance and Social Banking (*Nederlandse Vereniging voor Volkskrediet*, NVVK) and the Salvation Army (LIS 2009). Safe Houses organise meetings open to institutions not previously involved in any direct way in caring for juveniles at risk – for example childcare centres, playgroups, credit banks, the Salvation Army, and after-school childcare facilities – and their participation gives them a say in issues outside their traditional scope (Holvast & Bonthuis 2010: 32, 33). Increasingly, local authorities are making use of private camera surveillance centres to help maintain public order and safety. A quarter (24%) of all local authorities split the cost of security camera projects with private companies (Schrijenberg et al. 2009), turning them into a kind of 'deputy sheriff' (Torpey 2000; Lahav & Guiraudon 2000), in what is referred to as the 'nodal governance of security' (Rozemond 2010; Boutellier 2007).

Computerised 'professionalism'

One frequent aim of local authorities is to use ICT tools to generate management information. That is clearly one of the ideas behind the Juveniles Reference Index: it is also used locally to monitor processes and allow social workers to supervise one another's work (Keymolen & Broeders 2010; Keymolen & Prins 2011). Professionals can be instructed and processes or services evaluated according to productivity criteria, based on the management information generated by various databases, ranging from the public transport chip card to the Reference Index for Juveniles at Risk. The extent to which public servants and professionals are free to act (their professional autonomy) comes under pressure when the choices that they are expected to make relating to and on behalf of citizens, taxpayers, patients and so on are influenced and moulded by the automatically generated profiles constructed by government. Zuurmond has explored this trend from a sociological perspective and refers to it as 'infocracy' (Zuurmond 1994). Bovens and Zouridis (2002) refer to the shift of decision-making authority from the street-level bureaucrat to the screen-level bureaucrat and, finally, to the system-level bureaucrat. Zuurmond and Meesters (2005) suggest that in a networked environment, system-level bureaucrats are in turn elbowed out by chain-level bureaucrats – individuals with broad discretionary powers to decide on the design of a network's information systems and processes. Lyon (2009), in speaking of identification and ID cards, refers to 'stretched screens', an observation that also applies to the staff of the tax office's dial-up information desk and the national government's public information service, 'Postbus 51' (Office of the National Ombudsman 2010a). In their conversations with callers, these staff members are limited to the information that appears on their computer screen. All this puts pressure on professional autonomy, freedom of choice, and the human dimension, leading to more vulnerability 'at street level', which is precisely the level at which many public servants and other professionals who deal with government's ICT systems

(for example physicians working with the EPD) in fact do their work. The feelings of alienation that technology can create in the public apply equally to professionals, of course. This vulnerability is not rooted in a system's technical breakdown or malfunctioning, but rather in unpredictable 'breakdowns' within social contexts, where it has an unintended effect – dysfunctionality – or comes up against attempts by professionals to circumvent technology in order to prevent their metier from being hedged in by it (Van den Akker & Kuiper 2008). For example, alongside the 'official' medical dossiers that physicians are obliged to share through the national data exchange, they are also allowed to keep 'shadow dossiers' with more detailed notes.

The impotence of local authorities

The huge number of clever plans and ambitious targets often obscures the fact that many local authorities are struggling with eGovernment. For example, on 1 June 2010 11 per cent of local authorities had not yet joined the Municipal Personal Records Database (GBA) system, even though use of this system had become compulsory on 1 January of the same year (Tweede Kamer 2009-2010a). In addition 32 per cent of those who had joined were not yet ready to be connected to the system, and 5 per cent of all citizens – i.e. 800,000 people – had been registered incorrectly. But local authorities also come up against questions relating to the traditional organising principles of public administration. The strong emphasis on customised digital service delivery causes tension in the municipal organisation because the everyday reality of client-centred working conflicts with traditional values and attitudes in public administration (Hoogwout 2010). There is also friction between digital support for client-centred services and the statutory regimes that deal with personal data. Client-centred services force local authorities to dismantle their data-management systems and develop a new organisational model, the 'middle office'. The middle office is supposed to mediate between the local authority's client contact centre (the front office) and the various back-office systems from which all necessary data must be retrieved. In addition to a great deal of financial and other misery and the ups and downs of systems development (Mom 2010), the introduction of the middle office has led, at a more fundamental level, to information being retrieved from the data warehouse for activities and tasks beyond those permitted by law, without any scrupulous discussion taking place.[22] Ultimately, a lack of available funding and expertise means that small and even some medium-sized local authorities are almost incapable of managing the complex technical and policy-related know-how needed to be transformed into eGovernment. But even larger authorities find this difficult: in the autumn of 2010, a crisis in the City of Amsterdam's ICT system jeopardised the transfer of benefits by the social services.

The most important reason for such problems identified in the CapGemini report *Puzzelen met prioriteit* (Puzzling over priority) (Van Duivenboden & Rietdijk

2005) is that eGovernment is regarded as a technological issue that should be the responsibility of ICT departments or operational management. Policymakers do not recognise the implications for society of utilising technology, and give no thought to the context. They find it difficult to explain the political discourse in a way that the 'techies' understand, while the ICT experts, in their turn, are incapable of providing technical specifications in a way that reflects the social and political context. Consultants quickly move in to bridge the gap between the two, according to both the CapGemini report and those interviewed for this book.[23] They also indicate that, too often, local authorities end up having to reinvent the wheel, and that there is little guidance either from national government or the Association of Dutch Municipalities when it comes to good commissioning practices. For example, the chairman of the Manifesto Group, Johan Hakkenberg,[24] is critical of the Jorritsma Committee, which advised on public services provision and suggested in 2005 that local authorities should be made the first point of contact of a reliable and authenticated portal to all of government from 2015 onward. This is the Answer© concept (*Antwoord*©, Jorritsma Committee 2005): "No matter which channel private persons and businesses choose – be it the single phone number, the municipal website, or the service counter at the town hall – they will always receive the same reliable answer to their questions, will know that their applications are being processed, or will be referred to another government organisation."[25] Drawing on his professional experience, Hakkenberg comments that it is completely unrealistic to expect local authorities to build up the huge digital knowledge database needed to provide such a service, let alone maintain and update it and communicate its contents to citizens through a single service desk.

No helping hand or guidance

Ultimately, local limitations have consequences for how the broader development of eGovernment is structured and democratically monitored. Regardless of the circumstances – be it a national digitization policy with some projects being supervised by national government, a national sector-specific policy in which systems play a supporting role, or a local authority's own ambitions when it comes to innovating and updating its information management systems – local government virtually always operates in a context of overlapping policy domains involving many different parties. That is precisely why it is so important, particularly at the local level, to pay attention to the broader context in which applications are created, to allocate responsibilities, and to make arrangements for proper monitoring. In reality, however, the enormous variety of local initiatives and the many public and private stakeholders involved make proper supervision, monitoring and enforcement difficult. Public safety is a driving principle at the local level, often at the expense of privacy. A case in point is the enthusiasm with which a Safe House Amsterdam staff worker greeted a computer search program called Topic View.

" 'Topic View is unique … Every day, it gives us all the information found in all the police files. Not only the official documents, but also Word files that the police have quickly put on the system.' Topic View also contains 'soft information'. 'Say someone drives a pricey car, but his family is in debt. In the past, we'd work on reducing the debt. Now, though, we look for the illegal source of income. An information specialist processes the available information and we then put out request for further information" (Holvast & Bonthuis 2010: 34).

There is little question of the Data Protection Authority actively supervising this and other local practices, however. The case of the Reference Index for Juveniles at Risk shows that two 'realities' are in fact emerging: the reality of the drawing board at the national level, where a system is defined and given a statutory basis, and the reality of the 'shop floor' at the local level, where both the technical system and the underlying information processes take shape. The issues considered at the national level and the concern shown about the impact on citizens scarcely play a role in the referral systems created on the shop floor. There, in particular, it is the driving principles that rule supreme (Keymolen & Prins 2011).

The question then is how much coordination and guidance are required from national government. The catalogue of struggles, determination to seize opportunities, fragmented applications and lack of democratic supervision is largely the product of the 'Dutch culture of public administration'. Decisions cannot simply be imposed on local authorities; it is difficult to influence them, and they often require administrative agreement, something that involves lengthy procedures. Although the Government has now taken on board the Oosting Committee's suggestions for improving inter-administrative supervision, local authorities often chart their own course in digitization and information processes (a more comprehensive EKD than the restricted one proposed by the Minister), or decide themselves on the pace at which they will introduce new technology. Many local authorities are still asking citizens to log in to their electronic services using a user name and password, even though such combinations should have been replaced on 1 June 2009 by the DigiD code (NUP 2008: 21-23). And some local authorities are still not working with the GBA, but using their own population records instead. The national government has attempted to guide and put pressure on local authorities by introducing various 'acceleration agendas' and other initiatives, but the Dutch system of government does not lend itself well to meeting the national authorities' digitization aims. In the meantime, an entire world of interlinked systems and information processes is developing at the local level. For example, all local systems for the Reference Index for Juveniles at Risk have been linked with one another via a national 'umbrella', so that warning signs relating to young people at risk can be shared throughout the country. It is therefore striking that the phenomenon of digitization scarcely figures, if at all, in the current debate about

the overhaul of the public administration system. For example, the discussion paper issued by the Association of Dutch Municipalities (VNG) – which bears the meaningful title *Thorbecke 2.0*[26] – does not devote even a single word to the influence of ICT on the Dutch system of public administration (VNG 2010). And although the Advisory Council for Public Administration (Rob 2010b: 25) does examine typical features of eGovernment, for example horizontalisation and fragmentation, it makes only one explicit reference connecting ICT/computerisation and public administration: local authorities' problematic knowledge gap when setting up their own interactive websites.

4.3 INFORMATION-BASED POLICING

4.3.1 STRATEGIC ORIENTATION AND PRACTICES

In recent years there have been many different national programmes intended to define the form and content of digitization throughout the police force: the use of biometrics to ensure more accurate personal records and profiling; smart monitoring of transit nodes (roads, ports, stations – known as nodal orientation[27]); the use of open sources of information such as Facebook and its Dutch counterpart, Hyves, for investigation purposes; and greater use of ICT to analyse and enhance information. These programmes once again show a desire for prompt, forward-looking action and, notably, prevention: "The transition from information-driven *investigation* to information-driven *policing* will be continued", according to the Board of Chief Commissioners in 2005 (2005: 17). The individual local and regional police forces play a key role in implementing plans and achieving targets. But like the local authorities, the local forces are also struggling to keep up with the national targets and with their own autonomy as they implement projects and develop projects of their own.

There are numerous examples. The comprehensive approach to investigating and combating identity fraud within police systems is faltering, with police forces passing the buck when a citizen insists on having erroneous data removed (Buruma 2011). The notion of 'virtual moats' around cities, which made such a splash in the media when proposed a number of years ago, has virtually ground to a halt owing to problems encountered by local forces.[28] A study commissioned by the Police Academy criticises the 'nodal orientation' launched in 2005 by the Board of Chief Commissioners, concluding that 'front-line' police officers are struggling to meet the targets imposed on them from above in their daily work (Ferwerda et al. 2010). Progress has been made on monitoring roads, waterways and railway stations with a view to identifying large numbers of users, based on collaboration with non-police services and making use of advanced sensor and identification technologies. Nevertheless, the targets have turned out to be difficult to meet, according to the report, mainly owing to a stubborn focus on area-specific police

work and a lack of specific guidelines. In July 2010, the Minister responsible was obliged to tell the House of Representatives that some aspects of the police information management system were faulty. His conclusions were unmistakable: "Great risks have been taken when implementing the basic facilities, endangering the reliability and continuity of information provision. In that respect, there has been no improvement in the way the Dutch police forces operate at the local level" (Tweede Kamer 2009-2010c: 2). Interviewees who work for the police indicate that local forces are too often obliged to reinvent the wheel and receive too little guidance or support from the national authorities when faced with data processing and information quality problems. Examples range from the police force's participation in the Reference Index for Juveniles at Risk to its efforts to combat identity fraud. As regards the latter, local authorities and the police have been at odds for many years now about how best to tackle passport fraud. Local authorities want to provide the best possible service to citizens and replace lost passports as quickly as possible. The police, on the other hand, focus on law enforcement and crime investigation, and so advocate a more restrictive passport replacement policy. A similar dispute has arisen at airports, where the border police focus on control and the airlines focus on service delivery (Snijder 2010). Now that the biometric passport has been introduced, various stakeholders consider it vital for national government to offer more coordination and guidance in this area.

Box 4.1 The police and social media

The public's growing use of social media is also affecting how public actors such as the police and the Public Prosecutions Service operate. They are making considerable use of social networking media as a communication strategy or as a forum for their investigations. The initiative usually arises 'from the bottom up'. When the neighbourhood policeman uses Twitter, he makes himself visible on a communication channel that is an important window on the world for a growing number of 'clients'. Increasingly, the organisational risks involved in an informal approach of this kind are considered acceptable trade-offs for a more direct relationship with the public. Another social media strategy gets even closer to the essence of police work. Increasingly, the police and the public prosecution are asking the public to assist them in their investigations. Initiatives such as Burgernet ('Citizen Net', www.burgernet.nl) and the Hyves page maintained by the IJsselland police force (www.depolitiezoekt.hyves.nl) can be regarded as 'crowdsourcing' in police work. The downside of such initiatives is that they can generate a flood of useless tips; sorting through them then becomes part of the inquiry. Ed Kraszewski, a spokesperson for the National Police Service Agency (*Korps landelijke politiediensten*, KLDP), recently said in an interview that it took a lot of time to wade through all the information generated by police announcements, and that such information had not proved very useful in tracking down escapees.[29] He stated that his team sometimes got 'bogged down' in all the information.

The real information goldmine is not generated by the police force itself, however, but by unsuspecting Web users. Almost everyone leaves a digital trail of relationships, behaviour, locations and so on behind on the Web. When the police enter the digital realm, users – i.e. suspects, but other users as well – end up paying the price for the 'eternal memory of the Internet', where bits and pieces of their life course can be found. Almost every police force in the Netherlands has now joined the Internet Investigation Network;[30] which runs on stand-alone computers that the police use to track the movements and activities of people without them being aware of it. Social networking sites can also be 'harvested' on a much larger scale, without there being any specific reason for doing so. This functionality is one of the objectives of the Expertise Centre for Intelligent Data Analysis (KECIDA), a department of the Netherlands Forensic Institute,[31] which believes that the 'yield' harvested from such public sources is particularly promising. It is far from certain what requirements (guarantees) should be imposed on such activities: some critics say that 'systematic observation' calls for the same degree of caution and restraint in the digital world as in the physical one,[32] whereas others point to the public nature of the digital trails that people leave behind (Buruma 2011), implying that no special guarantees are necessary.

4.3.2 COOPERATION AND COORDINATION, PROVIDED THAT ...

The initiatives launched by the Dutch police have the same features as the projects discussed earlier:

- systems and data are rapidly becoming entwined and interlinked at the technical level, but there is no parallel allocation of responsibilities or move toward uniform requirements in the organisational and political-administrative sense;
- the information boundaries between policy domains (service, care and control) and actors (public-private) are becoming blurred;
- it is once again proving difficult to manage and coordinate along hierarchical lines.

The outcome is aptly expressed by the chief commissioners in their discussion of the use of private camera surveillance centres: "The question is whether this method offers sufficient guarantees of quality, integrity, democratic supervision and management in government control" (Board of Chief Commissioners 2009: 23). The 'spontaneously' and widely used Automatic Number Plate Recognition (ANPR) system serves as a good example. The police use this camera technology to enforce public order and investigate crime, comparing files on individuals under investigation, on stolen vehicles, and on unpaid fines with the data gathered through the ANPR systems. But it has not taken long for ANPR to be used for a whole string of other purposes as well: the police are also using it to tackle the problem of drug runners – a strategy that does not always have the approval of the courts[33] – and of groups of cross-border 'bandits' who operate in the Netherlands. It is also being used by the Ministry of Infrastructure and the Environment, in cooperation with the police, to monitor waste transport, by the

Transport and Water Management Inspectorate to check on transport by taxi and whether taxi drivers are taking legally required breaks, by RWS (*Rijkswaterstaat*, the executive arm of the Ministry of Infrastructure and the Environment) to control traffic flows, and by the Tax and Customs Administration to check up on various taxes (Tweede Kamer 2009-2010a; for earlier examples in other countries, see Bennett, Raab & Regan 2003). The absence of any special form of guidance or moderation imposed by politicians has led to enormous variety not only in the applications and, therefore, actors, involved, but also in the length of time that data is supposed to be retained. "The IJsselland regional police force stores the data for seven days, the Drenthe force for fourteen days … The Rotterdam-Rijnmond police force saves data for four months because ANPR is also used in crime investigations, for example drugs smuggling. Some forces retain data for even longer periods" (Brouwer-Korf Committee 2009: 68). After the commercial research firm Regioplan studied the value of using ANPR on the A28 motorway near the city of Zwolle and concluded that the system did indeed provide useful information for investigations, and that it also uncovered additional information that would not have emerged otherwise (Tweede Kamer 2010-2011f, 24-25), the Minister of Security and Justice, Ivo Opstelten, announced in December 2010 that legislation would soon be forthcoming. The proposal provides for retention of all data collected, be it data on 'suspicious' individuals or cars or on non-suspicious ones.[34] His announcement led MPs Gerard Schouw and Magda Berndsen (D66, democratic liberal party) to raise numerous questions, for example about the possibility of leaks and violations of drivers' privacy (Tweede Kamer 2010-2011g: 1-2).

4.3.3 FORGETTING

Ultimately, it is precisely the ability of the police – and, by extension, the courts – to gather information from a wide range of sources that has repercussions for the concept of 'forgetting' in the digital era and in eGovernment (Mayer-Schönberger 2009; Solove 2007; Buruma 2011). Technically speaking, the right to be forgotten and to 'start again' is virtually impossible for purported criminals who are branded as such on the Internet (Prins 2009: 119). It is in the nature of the Internet to save and copy, not to forget. Forgetting is also no longer technically necessary to free up storage capacity. Although legislation does prescribe time limits for storing data, the purging of databases appears to have little operational priority (Neuman & Calland 2007; Buruma 2011). In addition, people in many organisations and certainly those in investigation services are inclined to think that data may eventually come in useful at some point. For example, Choenni et al. (2011) conclude that the national police ReCognition System (*HerKenningsdienst Systeem*, HKS) – a database of the names of all individuals who have been reported to or booked by the police – contains 8,000 suspects, who are in fact deceased. In addition, the names of 2,800 individuals who have been cleared of all charges are still in the

system. Although these are only fractions of the total number of names in the database, the researchers recommend a more thorough screening of police systems for data contamination, especially since the police use these systems and others to construct risk profiles and because they are increasingly being interlinked. In an earlier study, Grijpink concluded that the computerised fingerprint system used by the Dutch police contained more than 101,000 cases of demonstrably fraudulent use of fingerprints (Grijpink 2006b).

Box 4.2 Ubiquitous memory: car keeps track of driving behaviour

Information technology is not just revolutionary in terms of *storing* data; it is equally potent in generating it. Every sensor and every chip generates output. That output has a specific function, but it can also be used for new, unanticipated purposes. Memory chips in cars are a good illustration. Most cars have diagnostic information systems that monitor the engine's performance. Known as On Board Diagnostics (OBD), such systems have been compulsory in most cars in Europe since 2001, for environmental reasons. The standard OBD system records the engine emissions, alerts the driver where necessary, and enables mechanics to trace problems. But car manufacturers are at liberty to build smarter systems with more functions and, consequently, with more memory. For example, certain makes of cars have what is known as an Event Data Recorder, which stores data on certain incidents, for example the speed the car was travelling before a collision. Garages find such data useful when servicing vehicles, but they have also been shown to be valuable in other situations. For example, in 2009 the Rotterdam police used a vehicle's event data recorder to find out the speed of a pick-up truck involved in a traffic collision in late 2009 that left four people dead. The recorder showed that the truck had been travelling at 147 kilometres an hour five seconds before the accident. Based in part on that information, the driver was convicted of reckless driving in September 2010. It took considerable technical ingenuity to read the relevant information, something that other police forces in the Netherlands are not yet able to do (*NRC Next*, 26 April 2010).

In practice, people are virtually powerless to correct an erroneous virtual profile. Apart from the fact that the police and the courts are slow to remove or overwrite information in systems, it is almost impossible for an individual to find out precisely what data is being stored on him or her, or where – a dilemma touching on the process-based principle of transparency. Requests to inspect information not kept in a criminal record but nevertheless stored elsewhere (logs, minutes of interviews with individuals who ultimately did not provide any useful information, reports on activities that did not produce results, etc.) are virtually never granted (Kielman 2010: 157; Buruma 2011). And although it is prescribed by law, there is no truly effective system for finding out what methods are being used against an individual, or what information is being kept on him or her (Buruma 2011). Another problematic issue is the right to correct data. It is not at all exceptional for someone who turned out later to have been unjustly suspected of a

crime – for example because of an administrative error by the police or the office of the public prosecutor – to remain coded in the system in such a way that the courts are reasonably likely to refuse him or her a Certificate of Good Conduct or a certain permit (Buruma 2011).

4.4 DESIGN AND MANIFESTATION

eGovernment is really put to the test at the local and operational level, i.e. by government agencies and by local or regional authorities. That is where applications are often built, either stand-alone or as part of a nation-wide system, and where systems have to prove their usefulness not only in interactions with 'clients' but also to those who actually employ them in their work. The same can be said of the underlying principles: the proof is in how they are elaborated and put into practice. Decision-making that is 'close to the people' has a certain value in this respect. Administrative agencies offer a good setting for building specific expertise, and local government is where local wishes and circumstances can best be taken into account. Nevertheless, diversity at the operational level can also unbalance the structure of eGovernment. The situations described in the previous sections suggest that sometimes the motto seems to be 'anything goes' (as with camera surveillance or the Topic View example given above). At the same time, voices have been raised in favour of more guidance and support. What this shows is that the variegated and sometimes chaotic picture of eGovernment that emerges at the operational and local level is often unintentional.

The driving principles of security, effectiveness and efficiency also dominate at the operational and local level. These are often thought to be decisive, and indeed, they often are. Sometimes, technological imperatives should in fact hold sway. After all, government does not operate in a vacuum: ICT-driven innovation offers many opportunities that cannot simply be rejected, and it has already made such inroads into society that government simply must keep up. One clear example of a technological and social imperative is government's duty to establish identities. That duty plays a role in the aforementioned need to achieve 'authentication at a higher level of assurance' than provided by the tools currently available. Identity documents have always been an important factor in social transactions, as it is not only government but also private individuals who require reliable identification in their dealings with others. The need for secure *digital* identity guarantees is equally urgent, simply because the digital world has added another layer to public life. The question then is whether government is bound to produce the technology that will solve the digital identity problems that are becoming more pressing all the time. In that light, the entrepreneurial role that the implementing bodies are taking – such as the RDW with its eLicence – provides a welcome impetus for tackling this government task. As noted before, multiple government organisations are vying with one another in this area to put 'their' solution 'on the map'. At the

same time, the entrepreneurial role that various public authorities have assumed in this area indicates that the situation has become unbalanced and rudderless. As countless examples illustrate, there is a plenty of leeway for public actors to pursue their aims, but also for private ones that want a piece of the action. Relatively few restrictions apply in this wide-open field.

The rise of the Safe Houses is a case in point. This is a significant development and one with far-reaching implications for the citizen: they are nodes for the most sensitive information, drawn from all kinds of different sources. Nevertheless, the Safe Houses arose spontaneously at the local level (Holvast & Bonthuis 2010) and they continue to operate without being subject to any special rules. They are not the only examples of developments in which a highly diverse group of actors are invited to come together and work 'behind the scenes' in areas previously unfamiliar to them. There is a great deal of confusion: the roles are divided on an ad hoc basis, in many cases without careful consideration, and proper frameworks are frequently lacking. Such confusion does nothing to promote policy effectiveness and efficiency – the reason the initiative was launched in the first place. ICT systems often run into serious problems: they do not, as a matter of course, fulfil what is often taken to be their promise, i.e. to simply make existing policy 'smarter' (to do the same, but better). The instrumentalist viewpoint sometimes obscures the magnitude of some undertakings, as noted above with respect to the Answer© initiative, which was supposed to be the apex of customisation. It is far from easy to develop and maintain a system that lives up to such high expectations, including those of the street-level bureaucrat. As noted several times above, communication between public administrators and system developers or between policymakers and government agencies about many eGovernment applications often resembles a Tower of Babel. In addition, inherent technological risks such as misinterpretations in data-mining or files that are unreadable in other ways have manifested themselves, without these problems leading to a genuine review of the relevant ICT systems and their interaction with users. The systems themselves can also suffer from communication problems. And they frequently do; otherwise, interoperability and semantic streamlining would not be such priorities. The way eGovernment is developing at the local level also shows that decentralisation comes at a cost, and that it is not always so efficient and effective to make local authorities responsible for rolling out the entire spectrum of applications because in many cases their organisations are too small to tackle the job properly. In addition, eGovernment would be considerably more expensive if every level was equally concerned about the quality of information. The example of the Tax and Customs Administration – which feels obliged to maintain a parallel personal records database because the proposed universal system, the GBA, is insufficiently accurate – speaks volumes.

eGovernment projects are far less likely to be built on the underpinning and process-based principles, and there is some hesitation about openly tackling the issues that these principles should bring into view. The most notable development, discussed several times above, is the breaking down of partitions between policy areas and of government organisations at the local and operational level, including those between the public and private sectors. These partitions are increasingly being regarded by both government and the public as impediments to effective action, but also as a barrier to a distinct identity: a unified government, approachable through a single service desk, is not a government with strict internal divisions. But as the process of 'departitioning' continues in order to promote a uniform identity (the one-stop service desk) and effective action (working in chains and networks), something is lost as well. Witteveen (2010: 219) describes the Weberian ideal type as follows: "Bureaucracy emerges in liberal societies that pursue freedom by separating domains from one another." Even with all their disadvantages, partitions encourage scrupulous, well-defined government action, and in doing so protect the freedom of the citizen. Citizens can develop autonomously – in other words, they can nurture personal freedom of choice and privacy – because they know that government organisations have been set up for a specific purpose and are not permitted to undertake activities beyond their narrowly defined duties and powers, even if those activities might otherwise be desirable. That demand, for a specific purpose for government action, is growing increasingly nebulous when it comes to information (as the rise of 'virtual organisations' such as RINIS demonstrates), and citizens must now be aware that when 'their' information falls into public hands, it may go on to lead a life of its own. Although government bodies have differing interests and objectives – the police and local government, for example, disagree about issuing replacements for stolen passports – they are increasingly utilising the same 'pooled' information.

4.5 CONCLUSION

All things considered, eGovernment has already overcome many barriers, but it has not yet begun to develop any notion of the broader and more fundamental consequences of digitizing and de-partitioning its operations. This conceptual void has a particular impact on the position of citizens and the level of protection they enjoy. There is often a misbalance between what ICT enables administrative agencies, local government and the police to do and what these same actors are undertaking to help the citizen keep up with the same process of digitization. Instead of the symmetrical empowerment of citizens, they are increasingly being asked to remain vigilant themselves and acquire new skills in order to compensate for the lack of transparency, and to cope with an increased burden of proof. The growing tendency of government to work in chains and networks has not inspired it to reconsider its responsibilities in the light of the citizen's position. The playing field that then emerges is one where the public authorities come up with creative

solutions and do their work with the best intentions, but where citizens are given little to go on in the longer term. The outlines of the new, ICT-driven operational reality have yet to emerge in the relationship between government and the citizen (individually and as a group). The playing field changes shape daily, and ostensibly by itself, but there is no sign yet of the institutional review that should accompany these changes. If all efforts remain focused solely on the array of opportunities, however, and the protective frameworks are ignored, the insidious weakening of the citizen's position will continue.

One urgent factor in this connection is that government has no overall strategic agenda or framework for 'forgetting'. If the rise of ICT has made anything clear, it is that forgetting no longer happens spontaneously. The gradual realisation that forgetting is a virtue (Mayer-Schönberger 2009) is tied to the observation that the quality of government information is not always what it should be, and that the citizen's right to privacy is gradually being undermined: if nothing is forgotten, then individuals can never break free of their past, and must remain wedded to the profile that government has created of them with the help of technology and information. The impact of 'images from the past' has been greatly increased by technology, especially because there is a tendency to pin people down on presumed identities which hinder their autonomy (freedom of choice), so to speak, from the inside. The same holds for the 'images of the future' formed by profiling. In short, a greater effort will need to be made to build underpinning and process-based frameworks for eGovernment, based on the realisation that forgetting serves a purpose (not only for citizens, but for government itself).

In the end, the lack of transparency and accountability on the operational side of eGovernment can only be rectified by government itself (and primarily by the national authorities), because it is impossible for individual citizens to penetrate to the inner circle of government information management without additional support and assistance. Assertive individuals who are aided by ICT can obtain and disseminate plenty of information about *policy*; they can even disseminate embarrassing policy or other government-related information (witness WikiLeaks) or generate it themselves (see Chapter 7). But the very same assertive citizens are often in a much weaker position when it comes to information pertaining to them as *individuals* – the type of information on which the decrees and decisions of eGovernment are based. The frameworks for transparency (citizens' position with respect to information) and accountability (citizens' access to and power to rectify and amend information) will not develop on their own.

NOTES

1 Directive 2006/126/EC of the European Parliament and of the Council on driving licences, OJ L [2006] 403, pp. 18-60.

2 Authentication involves demonstrating that someone is who he says he is (including by means of digital technology).

3 The Tax and Customs Administration, Statistics Netherlands (CBS), the Central Fine Collection Agency (CJIB), the Health Care Insurance Board (CVZ), the IB Group (IB-Groep), the Immigration and Naturalisation Service (IND), the Land Registry, Chambers of Commerce (KvK), RDW, the Social Insurance Bank (SVB), the Social Security Agency (UWV).

4 Interview with Prof. A. Zuurmond, founder of Zenc and co-partner in the firm; professor at Delft University of Technology; October 2010.

5 A sector consists of one or more organisations; if there are multiple organisations, they all work with a single service counter, the Sector Contact Office (SA). An SA ensures that data is delivered to or retrieved from the right source within the sector.

6 www.ocwduo.nl/klantenservice/privacy/privacy.asp.

7 Interview with Senators R.H. van de Beeten, H. Franken, J. Hamel, P.L. Meurs, I.Y. Tan, C.P. Thissen; May 2010.

8 *NRC Handelsblad*, April 2010.

9 A reference index is an ICT application that contains and shares notifications or alerts. It is used in particular in the care/youth care sector to allow various social workers and care organisations to communicate with one another. For a summary: CapGemini Consulting (2010b).

10 An interface consists of all collective arrangements made to enable two or more partners in the chain to share electronic messages.

11 A national exchange is a central node for data-sharing nation-wide (for example patient data) between local actors (for example care providers).

12 MEE is a consortium of organisations that support individuals who live with a disability, www.mee.nl.

13 "The survey revealed that more than 300 client data items were being used by two or more of the organisations for medical indication involved. Research shows that some of this data can be shared, but other data can not, for legal reasons. In order to remove the legal impediments, the Indication Dossier project will be continued in the form of a bill introducing the Data Exchange Act, coordinated by the Ministry of Social Affairs and Employment. The aim is to allow the organisations to optimise data-sharing between them" (Ministerie van SZW and Ministerie van VWS 2010: 7).

14 In 2010, the system consisted of 13 basic records databases with data on people, businesses, buildings, addresses, geography/maps, vehicles and incomes: the Municipal Personal Records Database (GBA), the New Trade Register (NHR), the

Basic Address and Buildings Database (BAG), the Basic Topographic Database (BRT), the Basic Land Registry Database (BRK), the Basic Vehicles Database (BRV), the Basic Wages, Employment and Benefits Database (BLAU), the Basic Incomes Database (BRI), the Basic Immovable Property Database (WOZ), the Database of Non-Resident Aliens (RNI), the Basic Large-scale Topography Database (BGT), and the Basic Soil and Subsoil Database (BRO).

15 www.e-overheid.nl.

16 In semantic interoperability, the context in which data is used is important, and it is accepted that the data can vary in meaning. See Wisse 2008.

17 The former president of the Netherlands Authority for the Financial Markets (AFM).

18 The ten criteria that were defined in 2005 by the Burger@Overheid.nl (Citizen@Government.nl) programme (Burger@Overheid.nl 2006) are: freedom to choose the communication channel; accessible government products; comprehensible facilities; personal information service; easy service delivery; transparent working methods; digital reliability; responsive governance; responsible governance; active engagement.

19 Interview with Mr J. Hakkenberg, Director of RDW, member of the board of the ICTU Foundation, chairman of the Manifesto Group, May 2010.

20 Interview with Mr H. Tankink, interim director of the BPR Agency, and Mr J.W. van Dongen, BPR Agency, November 2009.

21 Parliamentary Documents II, 2009/10, 29 362, 157 strikes an optimistic tone when presenting a range of projects; some of these fall under the National Implementation Programme on Service Delivery and eGovernment (NUP).

22 Interview with Mr H. Gardeniers and Mr E. Schreuders, Net2Legal, February 2010.

23 Interview with Mr H. van Duivenboden, B&A Consulting/Professor of Informatisation and Interorganisational Collaboration, Tilburg University, May 2010.

24 Interview with Mr J. Hakkenberg, Manifesto Group/RDW, May 2010.

25 www.antwoord.nl/.

26 Johan Rudolph Thorbecke (1798-1872) almost singlehandedly drafted the revision of the Constitution of the Netherlands in 1848, thereby limiting of the monarch's power, introducing direct elections, establishing freedom of religion, and increasing the power of Parliament and the ministers. The Dutch system of government is frequently referred to as the "House of Thorbecke".

27 Nodal orientation is an operational method in which the police look specifically at flows of people, goods, money and information. The police use the nodes created by the infrastructure of these flows as their point of action. See: www.politie.nl/Overdepolitie/Politie_in_ontwikkeling/Visie/Nodale_orientatie.asp.

28 The idea of screening every individual traveling on an access road into a city in order to filter out persons with malicious intentions is referred to informally as the 'virtual moat'.

29 Quote taken from a radio interview (Radio1 Journaal) on 9 September 2010.

30 http://230psporingsdingen.nl (consulted on 24 September 2010).

31 www.forensischinstituut.nl/producten_en_diensten/producten/kecida.aspx (consulted on 24 September 2010).

32 A website for police officers has this to say: "Legally speaking, whatever applies in the real world applies on the Internet too" (http://230psporingsdingen.nl, consulted on 24 September 2010).

33 The case law is inconsistent. See: NRC *Handelsblad*, 19 October 2010, p. 2 with an explanation by Ybo Buruma (NRC/NJblog, 19 October 2010).

34 *Algemeen Dagblad*, 8 December 2010.

5 EXCHANGE WITHOUT BORDERS

The setting up of information systems and the creation of connections between them have now become more or less the *lingua franca* of modern global governance. It is therefore obvious that information flows do not stop at national borders. As the WRR observed in 1998, information technology undercuts the significance of territorial boundaries. Today, governments are enthusiastically embracing that very feature. The global security drive after 9/11 has played a major role in this, but so has the extent to which the EU Member States have harmonised and coordinated their policies in a whole range of different areas. Information-sharing is important, after all, not only for security reasons; inside the external borders of Europe, it is also helping to complete the internal market and streamline administrative cooperation in many different forms. Although the Netherlands initiates and makes bilateral agreements governing data exchange (for example in 2010 with the United States relating to mutual access to one another's databases for fingerprint and DNA profile matching[1]), the way it uses technology and its attempts to expand information flows are influenced mainly by trends and developments at the European level. There are now a growing number of European databases in which personal data is circulated 'beyond the borders', and which are used as a basis for decision-making by administrative bodies in the EU Member States. The scope of these databases is expanding. Such European systems indicate a far-reaching level of integration: government at the European level is also, explicitly, evolving into eGovernment. A further factor is that the EU is also a source of legislation that sets the standard for national eGovernments. Domestic privacy law, for example, is largely derived from European legislation on privacy.

eGovernment applications and arrangements made at EU level have similar features to those at the national level, but their institutional setting is entirely different. Below, we analyse the nature of the EU's databases by looking at the roles and positions of the actors in this setting. The latter are not limited to the formal institutions of the EU, but also include the various actors other and bodies that influence European policymaking.

5.1 EUROPEAN INFORMATION DATABASES AND INFORMATION FLOWS

"Neither the Schengen area nor the EU internal market could function today without cross-border data exchange." Thus begins a Communication by the European Commission, published in mid-July 2010. The Communication presents "for the first time, a full overview of EU-level measures in place, under implementation or consideration that regulate the collection, storage or cross-border exchange of personal information for the purpose of law enforcement or migra-

tion management" (European Commission 2010a: 2-3). What is notable about the Communication is that the developments it describes primarily concern information rather than technology. The policy strategy that is presented focuses on information and provides a basis for reflection on "the possible need for developing a European Information Exchange Model based on an evaluation of current information exchange measures" (European Commission 2010a: 3). There is no doubt that innovations in hardware (storage capacity, computing capacity, speed, and portability), software (interactivity, Web 2.0), and other technical facilities (biometrics, RFID) also matter in European policy, but the implications of Europeanization, globalization and upscaling are most in evidence in cross-border information flows. The dozens of databases that have been introduced at the European level in recent years link Dutch citizens and their personal data – virtually – to the millions of people who live in the other Member States. The Member States and the US can make generous use of these databases, either directly or indirectly, thanks to a range of official rules, complemented by what is for most – including the European Parliament[2] – an unknown number of vague bilateral and informal agreements. Both the text of the Commission's Communication and its annexes reveal a cross-border digital 'lucky bag' of databases, with the Netherlands featuring, incidentally, as one of their major users (see Broeders 2009). And yet at crucial moments, there are gaps in the exchange of data, for example as revealed by a major vice case relating to child abuse at a day-care centre in Amsterdam in December 2010. The main suspect, an employee at the centre, turned out to have had a previous conviction in Germany for possession of child pornography, but because the European criminal records information system (ECRIS), agreed on in 2007, was still in the test phase in late 2010, his criminal record was unknown to the Dutch authorities. Nevertheless, empirical analysis of the situation in the Netherlands makes clear that data exchange generally does not stop at national borders. Thanks to globalization, the Dutch government's information policy is increasingly being dictated and organised at a higher order of scale, and indeed being implemented in international or Europe-wide applications and systems.

5.1.1 INTERNATIONAL SECURITY AS THE DRIVER

The key drivers behind the internationalization of information flows are the systems set up to tackle the problems of irregular migration, cross-border crime, and – in particular – international terrorism, a battle that the US has been waging and championing since the attacks in New York and Washington DC in 2001. National security, and the fact that immigration and security are now regarded as linked issues, rank as an important impetus for the new digital information flows (Lyon 2003; Zureik & Salter 2005; Boswell 2007; Guild 2009). Politicians and policymakers – including (and perhaps especially) those in Europe – have enormous trust in technology and are enthusiastic about the digital exchange of infor-

mation as the solution to these problems. Some years ago, a member of the European Parliament, Carlos Coelho, warned that citizens could become the victims of "an atmosphere of the 'impossibility of error' under all circumstances" (Liberatore 2005: 15).

Box 5.1 Technology points the way: European migration databases

A network of databases has been developed and introduced in Europe over the past twenty years intended to make migration 'manageable'. The new technology has proved to be enormously tempting in this respect: not one of the systems is still limited to the purpose for which it was originally set up. Indeed, the history of the migration databases shows that the design decisions taken in the first version of the application often deliberately accommodated the later expansions and additions that have taken place.

The Schengen Information System (SIS) rapidly became so popular that plans were laid to develop a SIS II system as far back as 1996. SIS II is still in the development phase, however, and over time the Member States have gradually added new items to their wish list; they wanted more information categories (biometrics, for example) and access to data maintained for new crime-fighting and counter-terrorism organisations. The European Commission has been extremely practical as regards these wish lists: pending the outcome of political decision-making, it has ordered the development of a system that satisfies all the requirements. The system "must be designed and prepared for biometric identification to be implemented easily at a later stage, once the legal basis, allowing for the activation of such potential functionalities, has been defined" (European Commission 2003: 16). The political decision adopted in 2007 concerning the functions of SIS II refers to fingerprints and photographs, but a research report by the UK's House of Lords has established that the system will also be suitable for iris scans and DNA profiles. The technical capability is already in place; what is required is 'merely' to create the necessary legal scope (House of Lords 2007: 20, n. 43). A similar expansion in functions can be found at EURODAC. Originally set up to combat 'asylum shopping', the EURODAC database quickly acquired a new purpose: to identify third-country nationals found illegally within the territory of an EU Member State. The ability to 'check' and identify people illegally residing within EU territory is an optional function, but rapidly grew so popular that when it evaluated the system, the Commission proposed storing the data on such individuals as well as just checking it.

Function creep is not only an issue when developing specific systems, but also when linking up different systems. The Visa Information System (VIS) has been designed for interoperability and synergy with systems that already exist or that are currently being developed. Right now, VIS and SIS II are 'separate containers', but in fact they share the same database and technical lay-out and the central databases are even at the same physical location. The technical design is entirely geared toward connecting the databases and allowing contact between differing information flows.

For a detailed description of these systems, see Broeders (2007; 2011b).

The European Union exerts an influence in two different ways. First of all, the Dutch government's own information policy has been shaped and – certainly with respect to security issues – dictated by various legislative measures taken in recent years at the European level. The Netherlands is naturally one of the negotiating parties in Europe, however, and that means that the EU's 'dictates' are not really imposed from above as much as Dutch politicians would sometimes like the public to believe. Striking examples include legislation on the use of biometrics in passports and the retention of data traffic records (telephone and Internet). The second way in which the EU influences national government is by means of truly European applications and systems. The resulting information flows are more European than national and are therefore usually discussed and adopted at the European level as well. Among the most notable examples are the numerous migration databases (Broeders 2007; Balzacq 2008; Dijstelbloem & Meijer 2009; Besters 2010; Besters & Brom 2010). Since 1995, the Member States have been working at the European level to develop a network of databases intended to support various migration policy aims. Foremost among these are the Schengen Information System (SIS) for registering and tracking irregular migrants and the use of false and missing identity papers; the EURODAC system, an EU-wide fingerprint database of asylum claimants to the EU meant to prevent 'asylum shopping' and ensure that asylum claims are dealt with in the country through which the asylum-seeker first entered the EU (known as the 'Dublin system'); and the Visa Information System (VIS), to be launched in a few years' time and consisting of a single, centralised personal data and fingerprint database of all those applying for an EU visa. The expansion of such European systems does not mean, however, that the countries connected to them have a single, uniform method for handling the data that they are to supply. In the case of both the SIS and Europol, it is clear that the participating countries do not all include (or exclude) the same data.[3]

5.1.2 DIGITAL EUROPE

But digital Europe is taking shape in policy domains other than security, crime-fighting and crime investigation. For example, the aim of establishing an internal market and allowing the free movement of people, goods and services increasingly requires a supporting information infrastructure. A cross-border electronic system has been set up to implement the Services Directive.[4] Known as the Internal Market Information (IMI) system, it provides for the smooth exchange of data between Member States for purposes of both service provision and monitoring.[5] On 3 August 2010, the European Commission released a video clip in which it proudly reported that the five thousandth organisation had been given access to this system.

The European Commission became active in eGovernment as far back as the 1980s and in particular in the 1990s (Kroon & Bekkers 1994). It began with the Delors

White Paper in 1993, which emphasised the importance and urgency of a pan-European information infrastructure for economic growth and competitiveness (Gomez-Barrosso et al. 2008). The year 1999 saw the launch of the eEurope programme (*eEurope - An Information Society for all*) as part of the Lisbon Agenda, which focused on making the European Union "the most competitive and dynamic knowledge-driven economy in the world by 2010" (European Commission 1999). The eEurope programme's main aims are the following: "bringing every citizen, home and school, every business and administration into the digital age and online; creating a digitally literate Europe, supported by an entrepreneurial culture to finance and develop new ideas; ensuring the whole process is socially inclusive, builds consumer trust and strengthens social cohesion" (European Commission 1999: 2). In order to achieve these aims, the EU would have to work on creating a favourable legal context and on supporting new infrastructures. The follow-up programme, eEurope 2005, interprets the aims in terms of higher economic productivity as well as improved and increased access to services for all European citizens (European Commission 2002). The i2010 eGovernment Action Plan promotes an open and competitive digital economy and emphasises the role of ICT as a driving force for social inclusion and quality of life; in addition, it prioritises creating a European information area without borders and encouraging innovation (Gomez-Barrosso et al. 2008). In some cases – specifically with respect to services targeting citizens and companies – it is not central government or the European Commission that is taking the lead in developing intra-European data exchange infrastructures; rather, governmental or quasi-governmental organisations at the national level are organising themselves into Europe-wide networks of similar national institutions in order to tackle the work of data exchange. Autonomous administrative authorities and agencies such as the RDW and the Land Registry are active in such networks.

"'Europe' facilitates such initiatives, but the new information flows and services are developing largely out of earshot of national and European public opinion. That means that this tangible form of European integration is, at best, evolving on the margins of public awareness.[6] There is one exception to the rule that most of the changes in care and service are coming from the bottom up: the European Commission's cautious steps toward building up a European infrastructure for identity management" (Stevens et al., 2010).

5.1.3 EXPANSIONISM

Anyone who examines the many European digitization initiatives will note that – like the Netherlands – the European Union is under constant pressure to expand the functions of these systems, to add more information categories to them, and to allow a growing list of authorities access to the data stored. That is true to a lesser extent for the systems used in the area of care and service (although on the website

for the aforementioned Internal Market Information System, the European Commission states that "the Commission is currently exploring with Member States in which other areas IMI can be used"), but it is certainly the case for the systems initiated in the areas of Justice and Home Affairs. For example, whereas the first generation of databases (SIS, EURODAC and VIS) focused mainly on 'problematic' groups of migrants – asylum seekers and migrants requiring an entry visa who pose a risk of irregularity – the second generation of European information systems has cast its net much wider (Broeders 2011). This second generation focuses on (1) all travellers worldwide and (2) using biometric data to check the identity of all travellers wherever possible (Broeders 2011; Hampshire & Broeders 2010). Passenger name records (PNR data) are compiled on all travellers, and the European biometric passport is being rolled out for all EU citizens who travel, although the Member States differ in the degree to which they store such data centrally (Böhre 2010). The EU is also debating a proposal for an EU-wide entry/exit system that – like the US Visit system – will register the biometric data of all people entering and leaving the territory of the European Union (Koslowski 2008; Hobbing & Koslowski 2009). Although there is – as yet – absolutely no legal basis for this proposal, it resurfaces again and again in all of the Commission's and Council's key documents. A series of conferences and feasibility studies in Brussels are preparing the groundwork for the next step in digitizing Europe's migration policy.

Such expansionism can be seen not only in the build-up of functions, but also in the swelling ranks of actors. It is not only Dutch policymakers and politicians who are interested in the data gathered in the private sector; there is also considerable interest in such cross-overs at EU level. And here too, the boundaries between the public and private sectors are becoming blurred: data is taken from the private SWIFT network (Society for Worldwide Interbank Financial Telecommunication) and airlines provide PNR data to the authorities in the United States, Canada and Australia (Mitsilegas 2009; De Hert & De Schutter 2008; Tweede Kamer 2010-2011e: 2). Work is now ongoing toward a more comprehensive EU scheme for providing PNR data on passengers travelling between the Union and all non-EU countries (European Commission 2010a: 20; Tweede Kamer 2010-2011e, 2-5). In the meantime, the EU and the US have once again locked horns over the precise scope of the agreements governing the exchange of both bank and passenger data.[7] Another example of government's interest in data gathering from the private sector is the Data Retention Directive mentioned earlier. Initiated after the terrorist bombings in London in July 2005, the directive obliges Internet and telecommunications companies to retain their customers' telecom traffic data records for a specified period of time and to make them available to government.[8]

One further dimension to this expansionist tendency is that national governments are exploiting the new European initiatives to go forward an extra step or two

themselves. One example is the EU regulation on the integration of biometric features in passports, intended to combat passport fraud and forgery. The Netherlands took advantage of this regulation, however, to set up a national biometric database that will also be used for crime investigation purposes (Böhre 2010; Hermans 2010), much in the way that the RDW intends to use the Driving Licence Directive to turn the driving licence into an electronic ID. The national database ran into political difficulties owing to increased public awareness of the associated risks, and has since been scrapped. The government stopped storing the data in July 2011 and is looking into the proper way to delete the records that had already been stored. Another example from several years ago is the process leading to the Requisitioning of Data Powers Act (*Wet bevoegdheden vorderen gegevens*). This legislation, which entered into force in 2006, was the result of EU agreements in October 2001 intended to improve legal cooperation between the Member States in order to combat organised and financial crime, more specifically money-laundering.[9] The process of adopting the protocol was speeded up after 9/11, and in the final version gives judicial authorities the power to demand the release of data from financial institutions. Before then, banks were able to decide for themselves whether or not to provide such data (MacGillavry 2000). The Dutch Government used the new European protocol as a vehicle for adopting a large number of far-reaching proposals put forward by the Mevis Committee, which had studied whether the Dutch Code of Criminal Procedure (*Wetboek van Strafvordering)* still offered a satisfactory legal framework for obtaining third-party information in criminal investigations, particularly in the light of new developments in ICT (Mevis Committee 2001). As a result, the legislation passed in the Netherlands is not limited to financial crime, but covers every sort of offence. It provides for a set of sweeping measures: investigating officers may also requisition all manner of identifying data on non-suspects in the interests of their investigation. In certain situations, moreover, they may also requisition 'future data', meaning that data generated during an upcoming four-week period – including any 'real-time' data – must then be passed on the judicial authorities.

5.1.4 SCANT DEMOCRATIC SUPERVISION

The European Data Protection Supervisor has warned repeatedly against the almost innate desire to expand and accumulate, the tendency to merge issues and, in doing so, to combine security and migration policy, and the inclination to overestimate the reliability of technology, in particular biometrics (EDPS 2006). The European Parliament has also repeatedly criticised information gathering and data exchange efforts in the area of Justice and Home Affairs, but until the Lisbon Treaty entered into effect, it did not have the formal authority to exercise democratic supervision. The Council of Ministers usually 'took note' of the EP's objections without amending the proposals to which they pertained.

The national parliaments, until recently the watchdogs of European democracy in issues related to Justice and Home Affairs, have been generally ill-informed about the substance of the proposals and the timing of the policymaking process in Brussels. For example, the Member States' parliaments have had virtually no influence on the development of the Justice and Home Affairs databases. The international procedure that led to biometric standards for passports being set by the International Civil Aviation Organization (ICAO), the negotiations with the US, and the decision-making in the EU that preceded the Dutch legislative process all took place almost entirely beyond the reach of Dutch democratic supervision (Böhre 2010; Broeders 2011), even though it was these procedures that defined the main standards for determining the path dependence of the Passport Act. Opinions differ as to who is responsible for this absence of informed parliamentary supervision. Some national MPs have expressed disappointment at the failure of their European counterparts to be more critical: former Dutch Senator Erik Jurgens (Labour Party) once mused that the problem with the European Union was that the European Parliament had too few members who were intrinsically vigilant about human rights, meaning that they seldom expressed strong opinions on the matter. Jurgens feared that in those areas where the EP had become active, for example on the subject of data retention, its concern had more to do with the economic interests of the providers affected and less with the privacy issues involved (Jurgens 2005: 98). It sometimes seems as if politicians in The Hague have also become all too accepting of Europe's ambitions, however: "Compared to the critical attitude of the Dutch parliament with regard to the establishment of SIS I, the development of SIS II was discussed only marginally. On the few occasions when the Senate or the Second Chamber of parliament made an inquiry about SIS II, they rarely raised fundamental questions" (Brouwer 2008: 452). The Dutch Parliament has occasionally been quite critical, for example with respect to the retention period for telecom traffic data records. On other occasions, however, it has meekly followed the European example, for example by allowing limits to be set on legal protection related to cross-border data exchanges in VAT investigations (Schenk-Geers 2007: 477).

Nevertheless, there are signs that Brussels is starting to rethink the ever-expanding and, in particular, increasingly networked European data systems. The Lisbon Treaty has 'normalised' policy in this sense: the European institutions will now operate in the traditional manner, meaning a stronger role for the European Parliament and the European Court of Justice. The post-Lisbon EP has already flexed its muscles in its discussion of the SWIFT agreements between the EU and the US – agreements which it ultimately rejected.[10] In interviews, the European Data Protection Supervisor Peter Hustinx[11] and the European legal expert Mitsilegas (Queen Mary, University of London)[12] pointed out that the new institutional framework would perhaps have a defining and qualifying influence on the policy content. The European Ministers of Justice and Home Affairs would no longer be

able to take decisions behind closed doors. Just what such greater openness will result in is naturally uncertain as yet.

5.1.5 EUROPEAN INTERESTS ARE LEADING

Digital service provision (both commercial and public) was at the top of the European agenda in the 1980s and 1990s, with EU projects aimed at facilitating Electronic Data Interchange (EDI) succeeding one another in rapid succession (Mitrakas 1997). In the past decade, however, security has arguably been the most important driver for expanding European information exchange systems and for harmonising the Member States' various measures, largely owing to the urgency attributed to this area of policy. Few officials at the European level are asking whether these measures have in fact improved security, and when they do, no answer is forthcoming. That is not only because it is difficult to say how many terrorist attacks have been prevented, but also because there is often no material on which to base a proper evaluation. For example, Europol's reports in no way establish whether police cooperation and cross-border exchanges of police data are effective counter-terrorism strategies and whether they should be expanded in future (Fijnaut 2007: 137).

But the European digital agenda is moving full steam ahead on more fronts than security. The coupled principles of effectiveness and efficiency also play a prominent role. For example, the European Commission concluded in January 2000 that certain forms of transparency and legal protection developed by some Member States within the context of exchanges of fiscal intelligence were incompatible with the growing demand for efficient information-sharing (Schenk-Geers 2007: 5). Effectiveness and efficiency (in the form of cost-cutting and improved access) are also the main drivers behind the growing European interest in interoperability. Simply speaking, interoperability means the ability of systems to 'talk to one another', i.e. to communicate and exchange data while avoiding data loss. The 2004 European Interoperability Framework makes policy recommendations relating to the technology and the information content on the one hand and the interaction between Member States' government information systems on the other. Initially, the priority was to arrive at a pan-European standardisation of eGovernment applications in the areas of service provision and care (for example by setting up pilot projects); these ranged from electronic toll charge systems and e-procurement to electronic signatures and digital patient dossiers (Ducastel 2008: 289). Now, however, the Union also wants the Member States to make police systems interoperable (Verbeek 2010: 34), and it is broadly promoting inter-sector interoperability.[13] These requirements move interoperability beyond the realm of effectiveness and efficiency. Discussions in the European Parliament show that the policy issue of interoperable national police databases is related directly to security objectives, making it a politically sensitive issue (De Hert 2006). The fact that

important treaties such as the Prüm Convention ('Schengen III') and the Hague Programme emphasise interoperability and the need for data exchange reveals the great political importance attached to information flows for security and investigation purposes (Broeders 2011).

Still, the underpinning principles, and in particular privacy, appear to be emerging from the European shadows. In January 2010, EU Justice Commissioner Viviane Reding noted the importance of data protection. She stressed the need to have a single legal framework for data protection at EU level for both the private and the public sector, including for police and judicial cooperation. The framework should give priority to transparency and ensure that individuals have control over their own data. The role of the data protection authorities should also be strengthened (Reding 2010). Six months later, the European Commission acted on this by publishing the above-mentioned Communication relating to information management in the European Union. In addition to presenting an overview of all existing EU-level instruments, the Communication sets out the main principles to be taken into account when dealing with personal data for law enforcement or migration management purposes. Alongside the familiar principles of privacy, necessity and subsidiarity, these principles include accurate risk management (risks should be based on evidence and not just on hypotheses), bottom-up policy design (the development of new initiatives must, at the earliest possible stage, draw on the input of all relevant stakeholders, including national authorities responsible for implementation, economic actors, and civil society), review and sunset clauses, and a clear allocation of responsibilities. What is striking about the latter is that the Commission says nothing about a clear allocation of responsibilities in the event that a citizen becomes entangled in the digital European world, but only cites this principle with respect to budgetary excesses and delays caused by shifting aims and conditions: "The experience of the SIS II project demonstrates that a failure to define clear and stable overarching objectives, roles and responsibilities early on may lead to significant cost overruns and delays in implementation" (European Commission 2010a: 30). Whether the underpinning and process-based principles will in fact be accorded a fully-fledged role in setting Europe's digital agenda is difficult to say right now. What is certain is that the general framework for data protection will be reviewed starting in 2011, and that decisions are expected to be taken in that regard. On 4 November 2010 , in order to prepare for this discussion, the European Commission presented its "strategy to strengthen EU data protection rules", which includes proposals for updating these rules. The Commission states, for example: "People … should have the 'right to be forgotten' when their data is no longer needed or they want their data to be deleted" (European Commission 2010c: 1).

5.2 CONCLUSION

Connectivity does not stop at national borders. The rise of ICT involves scale advantages that open up new policy options at the European level which are literally beyond the reach of individual Member States. By sharing information, the EU Member States can tackle issues that would have otherwise been unmanageable. After all, a common migration policy that is truly harmonised in operational terms (and not merely with respect to legislation) would be unaffordable without European migration databases. Recently, the original focus on asylum seekers and irregular migrants has been widened to encompass all travellers. The fact that information-sharing is now being considered for the internal market demonstrates that the information society is reaching maturity. But there is clearly no sharp distinction between the aspects of eGovernment for which the EU should be responsible and the aspects for which the Member States retain competence.[14] The European Union is in any event devoting itself enthusiastically to eGovernment and can only be expected to continue along that path.

An even balance between driving, underpinning and process-based principles is also important at the European level. Migration databases are truly European applications, and the individual Member States can do little to right the balance there. In other areas, however, such as the EU's privacy legislation or the Regulation[15] relating to the introduction of biometrics in passports, the structure is more layered and national implementation can still tip the balance in either direction. It is clear from the various European initiatives that the EU also has trust in technology and in the benefits of information-sharing. The basic principle, which often remains unspoken, is that the more data that is exchanged, the better the combined European governments can meet the many challenges facing them. One of those challenges stands head and shoulders above the rest: to protect the citizens of Europe against the threat of terrorism. The European Parliament has consistently shown that it does not agree with such blanket assumptions, for example by stepping on the brakes in discussions about data exchanges with the United States. Until recently, however, it often had neither the opportunity nor the authority to influence the tenor of the debate, let alone the relevant proposal. There is therefore constant pressure to expand the existing European applications, with new information categories being added and new national and European organisations joining in.

ICT may indeed have opened up unprecedented opportunities for policymaking at the European level too, but the benefits of such policy are extremely difficult to identify. The paucity of evaluation noted in the Dutch context can also be seen within the EU. As a result, efficiency, effectiveness and security have become somewhat elusive concepts. As in the Netherlands, the success of an initiative in Europe is measured on the relevant system's own terms, for example how many

unwanted aliens have been flagged in the SIS system. On the other hand, citizens whose data has been entered into one of the European databases – and more and more of them are simply 'normal' citizens – are in an exceptionally weak position. They do not even know that such databases exist until a national authority turns down their application or takes some other negative decision based on a piece of digital 'European' information – and such an entry is exceedingly difficult to have reversed or deleted (see the Office of the National Ombudsman 2010c). The responsibility for righting errors or correcting faulty information is based on the 'historical' principle: the organisation that originally recorded the information – even if located in another Member State – must make the correction. This has resulted in an impenetrable legal protection 'system'. In the 'database state', the underpinning and process-based principles are even more problematical at the European level than at the Dutch national level. This is a worrisome development, especially with European applications growing ever-wider in scope and – viewed from the perspective of the average citizen – affecting everyday life more and more.

One final comment is that 'the' European government wants not only to be a user but also, very clearly, a driver of ICT by encouraging not only the ICT industry but the use of ICT in society in general. That makes the input of commercial stakeholders highly important, even to the point that they are invited to help design public applications. The privacy settings for the eCall initiative, for example, are purely the result of public-private cooperation. Although such cooperation may increase an application's chance of success, it does give rise to the paradoxical situation that government is sometimes merely the facilitator even of its 'core business', i.e. regulation.

NOTES

1 The agreements were laid down in the Prevention and Combating of Serious Crime (PCSC) Agreement, which at the end of 2010 had yet to be submitted to Parliament for approval. *Nederlands Juristenblad*, 2010, pp. 2731-2732.

2 Interview with S. in 't Veld, Member of the European Parliament, January 2009.

3 *NRC Handelsblad*, 17 December 2010.

4 Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market, *OJ* l 376, pp. 36-68.

5 Decision 2008/49/EC of the European Commission of 12 December 2007 relating to the implementation of the Internal Market Information System (IMI) as regards the protection of personal data, *OJ* l 13, pp. 18-23.

6 Interview with Constantijn van Oranje, office of European Commissioner Neelie Kroes, Brussels, 24 March 2010.

7 *NRC Handelsblad,* 20 December 2010.

8 Directive 2006/24/EC, *OJ* L 105, pp. 54-63.

9 Treaty Series of the Kingdom of the Netherlands [*Tractatenblad*] 2001: 187.

10 The SWIFT agreement gave the US access to European bank data for counter-terrorism purposes. Serious concerns about privacy, proportionality and reciprocity led to the European Parliament rejecting this agreement.

11 Interview with Peter Hustinx, EDPS, Brussels, March 2010.

12 Interview with Valsamis Mitsilegas, Professor of European Criminal Law at Queen Mary, University of London, May 2010.

13 Decision 2004/387/EC of the European Parliament and of the Council of 21 April 2004 on the interoperable delivery of pan-European eGovernment services to public administrations, businesses and citizens (IDABC) , *OJ* l 181 (2004) pp. 25-35. The decision refers to 'horizontal' interoperability.

14 In other words: we need not expect a battle over whether the EU is authorised to involve itself in aspects of eGovernment. What is still uncertain, however, is whether the European level is really the most suitable for specific initiatives. In the view of the Dutch Government, that is certainly not always the case (Tweede Kamer 2010-2011c).

15 Council Regulation (EC) No. 2252/2004 on standards for security features and biometrics in passports and travel documents issued by Member States, *OJ* L 385, pp. 1-6.

6 MARKET MASTERS AND MASTERING THE MARKET

Without an ICT supply market, there would be no eGovernment. On 9 September 2010, the then Minister of Health, Welfare and Sport, Ab Klink, reported to the House of Representatives on the sums spent on eGovernment, in this case on the EPD, in the ICT market.

> "In July, the Ministry received a request under the Government Information (Public Access) Act from RTL Nederland[1] asking for a full accounting of 'all costs incurred and activities carried out under the auspices of the Ministry of Health in connection with the EPD for which invoices have been sent or which have been paid for, other than the Ministry's regular, official costs and activities'. Between 2002 and 1 July 2010, a total of EUR 217.5 million was spent on activities related to the introduction of the national data exchange infrastructure in the healthcare sector (including audits, advisory studies, pilot projects, communication, IT, development and management, project management and Nictiz[2] institutional and project funding)" (Tweede Kamer 2009-2010g: 10).

Conversely, the ICT market would never have grown to its current size if eGovernment had not taken off to such an extent. In order to achieve its ambitions and carry out all its plans, government leans heavily on a wide variety of parties that operate outside the public sector. The relationship between government and the ICT market has developed along three lines. The first is economic: the ICT industry is an important sector, and government is a crucial partner for the companies that operate within it (system engineers, developers of data and information applications, consultants). The second line is administrative. The ICT industry functions as an extension of public administration: government implements policy by means of ICT applications, and must therefore depend, at least in part, on the suppliers of those applications. The final line is regulatory. By regulating the ICT market, government forces companies in the sector to conduct their commercial affairs in a particular way. For example, it can decide to enact and enforce certain rules because a small number of market parties have acquired so dominant a position in informational terms that public interests are at risk.

6.1 eGOVERNMENT AS ECONOMIC FORCE

6.1.1 PURCHASING WITHIN eGOVERNMENT

ICT is a dynamic and sizeable sector of both the Dutch and the international economy. In 2007, the top 250 international ICT firms recorded turnover of USD 3.8 trillion. The sector as a whole also drives innovation. It invests much more of its earnings in R&D than the automobile or pharmaceutical industries, both of which are traditionally regarded as heavily dependent on new discoveries and innova-

tion. Worldwide, the ICT sector invests USD 130 billion in R&D; 25 per cent of this comes from companies based in the European Union (all figures taken from OECD 2008). In other words, the ICT industry is a dynamic force – innovative, a driver of economic growth, and a source of skilled jobs. Government is therefore keen to 'nurture' this robust, valuable industry cum knowledge sector. In addition, ICT also generates the necessary energy and innovation in the social arena, which is why the Dutch Government made a EUR 54 million investment incentive available in 2008 for "sector-specific ICT projects in social sectors."[3]

The public authorities are themselves major purchasers of ICT products. Many of the numerous eGovernment projects undertaken by local, national, European and international authorities are ultimately developed and carried out by ICT firms, whether or not chosen by tender. In 2007, the Ministry of the Interior and Kingdom Relations reported that between 2000 and 2013, the national government (including independent agencies) will have built up a portfolio of ICT-related projects worth EUR 5.8 billion, of which EUR 4.1 billion will ultimately be spent directly on ICT (Netherlands Court of Audit 2008a). This did not give the Netherlands Court of Audit (2008a: 29-30) enough information to estimate annual expenditure, however, and it in fact wondered whether the actual sum spent had not been higher than reported. In the UK, estimates from five years ago put spending on public-sector ICT at some GBP 14 billion a year (Dunleavy et al. 2006). These impressive figures indicate that the public-sector ICT market is not only the result of demand-pull; technology push also plays a role. As key commercial parties, ICT firms actively 'work' the market, sometimes with the support of an ICT consultant. Even government is not immune to the occasional 'solution in search of a problem' in terms of a new technology or type of application. In interviews, representatives of CIO Platform Nederland indicated that government – like business and industry – had been backed into a corner by a very small number of large ICT providers, and had little idea of how to deal with this situation.[4] According to these CIOs of large corporations, there is every reason for government and other businesses that are similarly dependent on ICT suppliers to collaborate in order to improve commissioning practices.

One part of the public-sector ICT market is to be found within the ministries and agencies themselves and relates to internal matters, for example salary systems, archiving systems, security, and keycards. Another part, however, relates either directly or indirectly to government's interaction with the citizen. Many dozens, if not hundreds, of applications have been developed in recent years in the policy areas of service, care and control. Most of these were designed and built in close cooperation with the private sector (Ministerie van EZ 2008). The tender specifications are sometimes worded so broadly that the external party eventually awarded the contract is able to choose the government actors that will be invited to help develop the application.[5] In some cases, market involvement is motivated

by more than the specific assignment alone; the private actors have their own agenda. One example is eCall, the EU project that involves fitting cars with electronics that emit an emergency signal (either manually operated or automatic) in the event of an accident. The European Commission is counting on the eCall project to significantly reduce the number of traffic fatalities on Europe's roads. The eCall system also gives the national road management agencies an excellent tool for optimising traffic management operations, for example to reroute traffic around an accident site or to instruct road inspectors on the spot. The national authorities are considering applications beyond traffic safety as well (for example crime investigation), and a variety of private actors – including the car industry, mobile telecommunication operators, private emergency services, and insurers – are encouraging the development of eCall in order to increase their earnings, develop new products, or streamline existing services (Potters & De Vreeze 2010).

The biggest 'growth market' for ICT and other technological applications is the security market. Since 9/11, the market for databases and for biometric and other internal security systems and applications has been booming. In a study published in 2004, the OECD referred to the 'emerging security economy' (Stevens 2004); Hayes (2009) calls it the 'growing Homeland Security market'. However one defines it, it is in any event clear that these are growth markets and that companies operating in them are actively marketing their products. The 2004 OECD study estimated that the security economy was worth about USD 100 billion (Stevens 2004). On a somewhat smaller scale, the International Biometric Group expects the market for biometrics to increase from USD 3.42 billion to USD 9.37 billion between 2009 and 2014. It has also predicted that, owing to the financial crisis, most of that market will consist of government contracts (*Biometric Technology Today* 2009: 11). The market for biometrics has a number of notable features. Spectacular growth forecasts have made this an international and highly competitive market, but it is also a relatively new one that in many cases has yet to establish uniform standards and reliable products. Snijder (2010) shows that the international biometrics industry is sharply divided into national segments, with innovation being largely in the hands of the major biometrics companies (there are approximately six such companies worldwide).

"Improvements in interoperability would not benefit the market position of these major companies, which – owing to their intimate relationships with public-sector customers and the limited interchangeability of their products – are certainly not eager to welcome market newcomers. And because innovation costs a lot of money and newcomers to the biometrics market are unlikely to be awarded big government contracts, there isn't much strategic technical innovation. The market leaders do innovate, but within the scope of their own technology" (Snijder 2010: 55-56).

In late 2010, the House of Representatives grew concerned about reports that the Minister of Justice had awarded the contract to construct the national biometrics database to a 'commercial French firm' following a tendering procedure.[6] Several of the political parties were worried that, according to MP Pierre Heijnen (Labour Party/PvdA), "central storage could also automatically fall into foreign hands" (Tweede Kamer 2010-2011a:3). Said MP Ronald van Raak (Socialist Party):

> "I would think it is entirely logical that a Dutch passport should be produced, managed, issued and monitored by the Dutch government. However, there is little about the Dutch passport that I hold that is still truly Dutch. Its production has been contracted out. It is produced by a commercial French firm. The fingerprint that it contains is entered into a database, and that database is also managed by a commercial French firm. There are commercial interests involved and the intelligence service AIVD[7] has warned that this was not very clever, that contracting out databases, sensitive information can be dangerous. I'm sure the AIVD has a good reason for issuing that warning" (Tweede Kamer 2010-2011a: 3).

In response to this discussion, the State Secretary reported that, with respect to the central database, no irreversible steps had yet been taken (Tweede Kamer 2010-2011a).

In addition to the technology market for developing technological applications, there is also an equally profitable information market. The gathering and processing of information for sale, or the utilisation of information for targeted advertising, is a highly lucrative business. Google, the uncrowned king of personal data collection, linking and enhancement for advertising purposes, reported turnover of USD 6.77 billion in the first quarter of 2010.[8] The information market is also valuable to government, not only because companies are commissioned by the public authorities to feed databases, but also because government has long been making eager use of the wealth of information collected in the private sector.

6.1.2 THE ICT 'MARKET' WITHIN GOVERNMENT

eGovernment is not being constructed by commercial parties alone, however. It is also being developed within government itself. One of the core tasks of the National IT Institute for Healthcare in the Netherlands (Nictiz), for example, is "to develop and select the specifications for the national generic healthcare infrastructure and the EPD (including the standards to be upheld)" (Pluut 2010:14). The most important development agency within government is the Netherlands ICT Implementation Organisation (ICTU), set up by the Ministry of the Interior and Kingdom Relations and the Association of Dutch Municipalities (VNG) in 2001 to develop large and small ICT projects for public authorities (Van Loon 2010). Along-

side these and other public-sector ICT developers, however, are a range of commercial firms that frequently work inside the walls of government on constructing eGovernment (Horrocks 2009). Large numbers of commercial developers and external consultants are contracted to work on many of government's ICT projects and to assist large agencies such as the Tax and Customs Administration. An article published in the online magazine *webwereld.nl* which revealed the relative numbers of public servants and external ICT professionals working for the Ministry of the Interior and Kingdom Relations – the information was requested under the Government Information (Public Access) Act – was given the suggestive and meaningful title 'National government ICT is a Valhalla for hirelings'.[9] Even ICTU's own workforce consists largely of external professionals. According to the ICTU, this allows the organisation to expand or contract with the supply of work.[10] What that often means in everyday practice is that the civil servant responsible for an ICT project within a Ministry does business with an external project manager who has excellent technical credentials and can make a large team available. In other words, the expertise on the two sides is far from evenly balanced.

6.2 THE ICT MARKET AS AN EXTENSION OF PUBLIC ADMINISTRATION

6.2.1 PROBLEMATIC COMMISSIONING PRACTICES

Close, professional supervision of developers has turned out to be difficult in many eGovernment projects. That is partly because government's technological expertise is limited, but it is also because its ideas relating to commissioning and its commissioning practices are not always as professional as they might be.[11] In late 2010, for example, the Ministry of Justice cancelled its Caijs ICT project, meant to serve as a prison information system for the National Agency of Correctional Institutions (*Dienst Justitiële Inrichtingen*, DJI). The project, which had already cost EUR 12 million in 2009 and 2010, was cancelled because too many aims had been defined, making it unmanageable.[12] Earlier ICT projects – among them C2000, Walvis, and the Surcharges project at the Tax and Customs Administration – had also run into major problems. The former National Ombudsman, Marten Oosting (now a member of the Council of State), had the following to say about the Walvis project: "In the case of Walvis, either we were all overly enthusiastic or the legislator simply ignored any cautionary advice" (Februari 2008: 91).

Various reports by the Netherlands Court of Audit reveal considerable room for improvement with respect to the costs, scheduling and efficiency of ICT development projects.[13] The Court of Audit has commented that projects are often overly ambitious and complex, and that this quite often leads to excessive costs and delays and to results that do not always live up to expectations (Netherlands Court of Audit 2007a). The same observation can be applied both to large-scale Dutch

projects (Netherlands Court of Audit 2007a, 2008a; Snijders 2011; Pluut 2010) and to European projects such as SIS II or VIS (Broeders 2011). In 2008, based on 350 reports of 'ICT wastefulness', the Socialist Party drew attention to a wide range of problems, including tendering irregularities, conflicts of interest between government and the market, poor communication, megalomaniacal politicians, and a lack of expertise (SP 2008). In the spring of 2010, the Advisory Board on Administrative Burdens (*Adviescollege toetsing administratieve lasten*, Actal) sent a letter to the State Secretary for the Interior and Kingdom Relations reporting that a projected saving of EUR 500 million would not be feasible owing to the lack of structure in the deployment of ICT (Actal 2010).

One key factor in this problem is the visible tension between what 'street-level' agencies want from ICT and the systems that are actually developed by the policymakers at the relevant ministry. It is only rarely that the agencies – the end users – are invited to take part in the development process early on. Indeed, they are often left out of the process entirely, with a turnkey system being delivered – or, to put it less politely, tossed over the fence (Van Loon 2010). There is broad agreement – within the police, the Tax and Customs Administration, the partners in the Manifesto Group, and Logius – that agencies are too often left on the side-lines when systems and applications are being developed, and when they *are* allowed to contribute, they are brought in far too late. That means that there is often a huge gap between government (usually a ministry) as commissioning body and government as end-user of the resulting ICT systems and applications.[14] This discrepancy between policy objectives and practical implementation can also be seen in the process leading to the introduction of the biometric passport. The policy is being introduced long before the control infrastructure is in place that will be required to actually use the biometric passport at the border (Böhre 2010).

Moving up a scale to the digital borders of the European Union, we see that there is an even bigger discrepancy between the Union's policymaking on high-tech digital and biometric databases and the everyday work being carried out at the external borders of the EU.[15] Opinions differ at various levels of government and politics as to when a system is 'finished'. Especially when the lines of communication between the politicians and those working at the coalface are very long, the tendency is to define success or failure at the level of the system: if the system is up and running, the project is considered a success. That is often also the approach taken in evaluations. The few evaluations of the EURODAC system (designed to detect multiple requests for asylum in the EU) analyse the information flows and 'hits' between Member States, but say nothing at all about whether or how the information is used in relation to the aims of the system, i.e. to assist in the transfer of asylum seekers between the Member States. The logic of the system commands all the attention and defines the 'outcome' of the evaluation (Broeders 2011).

Part of the problem when it comes to public-sector commissioning practices is that government does not act as a single, uniform entity when setting the requirements for ICT. Indeed, the Netherlands Court of Audit has pointed out that it is precisely the political dynamic between a minister, the House of Representatives and the civil service that often leads to failure or delays in large-scale ICT projects. In a similar way, the dynamic relationship between the EU's Council of Ministers, the Commission, and – especially in the post-Lisbon era – the European Parliament generates constantly changing political demands on emerging systems, combined with unrealistic deadlines (Broeders 2011).[16] A further factor is that there is often a chasm between the ministries – usually the commissioning bodies – and the parties that build the systems. The Gateway Review of the NUP (mentioned earlier) seriously questions the quality of the ministries' commissioning practices: "When it comes to enormous projects such as these, there is reason to question whether government employees in general and those in the commissioning ministries in particular are well enough equipped for such tasks as project and programme management" (Gateway NUP 2009: 2). Some interviewees believe that there is too much emphasis on managing specific projects and too little emphasis on the overarching factors that affect the coherence of policy and implementation.[17] According to interviewees Peter Wijntje and Sjoerd Peereboom (Ministry of Finance/Tax and Customs Administration), factors such as the legal framework and more specifically the citizen's access to legal redress should not be left to project managers; they are matters that should be entrusted to public administrators. Focusing on individual projects and managing from a narrow operational perspective also blocks an organisation's ability to learn, they claim, and prevents it from developing a strategic agenda for the interrelationship of multiple initiatives.

The ICTU offers an apt illustration of these problems. Ministries often lack a solid understanding of the matter and are unable to define assignments precisely enough.[18] In terms of the success of large-scale ICT projects, it is certainly problematical that the ICTU is – in its own words – a genuine project organisation. Once a project has been completed, it is crossed off the ICTU's agenda (Van Loon 2010). But in many cases, the work of incorporating the project into the relevant organisation's everyday work has yet to begin. In addition, systems are never 'finished'; they will always need to be managed and require ongoing development. In 2006, a new organisation known as GBO.Overheid was set up to manage various eGovernment systems; it was later renamed Logius.[19] Logius in fact takes over where ICTU leaves off and manages systems on behalf of government. There is very little coordination between these organisations, however. It is only recently that the Ministry of the Interior and Kingdom Relations has tried to get the parties to collaborate and coordinate their work more systematically.[20] In this complex setting of commissioning, development, management, and ongoing development, who exactly is responsible for ensuring that the system is actually aligned with the

relevant policy objectives? After all, many choices are made in the course of programming, and are made repeatedly as time passes. In practical terms, it is not clear – or not sufficiently clear – who is monitoring accountability.

6.2.2 THE CHIEF INFORMATION OFFICER (CIO) AS PROBLEM SOLVER

Inevitably, a government that innovates and therefore takes advantage of the new opportunities offered by digitization for policy implementation is operating in an arena whose contours have not yet been defined. The path of digitization is therefore unavoidably strewn with both project successes and project failures. There is simply no innovation without risk. It is important to learn from both the successes and the failures, but that often fails to happen. Some years ago, the Netherlands Court of Audit advised the Government to introduce a new job title in national government to ensure better project management: that of Chief Information Officer (CIO). One of the CIO's duties would be to furnish Parliament with accurate, complete and timely information about the progress of ICT projects (Netherlands Court of Audit 2008a: 53). In the United States, where heads of government agencies are required to appoint CIOs (at the highest levels of the civil service hierarchy), there has been a vast improvement in project throughput times (Petri 2008). Governments in other countries, such as Austria and the United Kingdom, have also introduced the position of CIO. The Dutch Government followed up this suggestion and the Netherlands now has a Coordinating CIO (*Rijks-CIO*), responsible for coordination, as well as ministry-level CIOs. Various agencies and one local authority have followed this example (Snijders 2011). The Coordinating CIO is responsible for managing the work of the CIOs in national government. CIOs are supposed to advise senior public servants and political leaders on large-scale projects, either on request or at their own discretion. It is therefore important for the CIO and policymakers to have a good working relationship. One problem is the scope of the CIO's influence. Most ICT projects, especially the largest ones, are implemented within autonomous administrative authorities or other agencies that operate at some remove from the responsible ministry (Snijders 2011). CIOs also have no influence at regional or local level, even though large ICT projects – for example the Reference Index for Juveniles at Risk – often involve all the various administrative levels. In actual fact, CIOs mainly concern themselves with making ICT projects manageable, and scarcely have time to function as information strategists or trend watchers. That means that CIOs may end up bearing a heavy burden of responsibility without proper acknowledgement; at best, they exercise some authority, but they have no real power. In its Coalition Agreement, the Rutte Government (which took office in 2010) has in any event said that it will take systematic action to achieve closer supervision of large-scale computerisation projects and to solve problems with computer systems (Regeerakkoord 2010: 42).

6.2.3 POLICY AS SYSTEM DESIGN

Dunleavy et al. (2006: 61) view the Netherlands as a typical – albeit extreme – 'polder' version of the European Rhineland model when it comes to government's cooperation with ICT firms. The focus in this model is on 'a good relationship' and 'consensus and mutual support', unlike the Anglo-Saxon model, which emphasises outsourcing and financial control. When government, developers and advisers cooperate this closely, it is often difficult to see who is guiding the interplay of policy objectives and the design of the actual system. In those areas in which eGovernment is taking shape thanks to close interaction between government (the commissioning party) and the commercial market (developers and consultants), the ICT market is really an extension of public administration, with important administrative and policy decisions being taken or 'preprogrammed' at multiple points throughout the process of system development. This tendency has been reinforced by the recent popularity of Privacy Enhancing Technologies (PETs), which will be examined in the next chapter (Section 7.1) (compare Article 29 Data Protection Working Party and Working Party on Police and Justice 2009: 12). In PETs, the limits set on the technology are actually embedded into the applications. That means that government has to make clear in its instructions to system designers that privacy guarantees must be incorporated into the application via PETs, making its commissioning practices all the more crucial. But government frequently has other priorities. Experience has taught system engineers such as CapGemini to design software in a way that leaves room for an as-yet only vaguely expressed political wish to combine – or separate – information flows. The 'partitions' that the engineers then construct between information sources can be easily removed or reinforced if this is requested later. That prevents projects from running up unnecessary costs in the event of changing opinions or an altered political course.[21]

The interplay between system development and policy decisions is obvious not only at the national level. By choosing to allocate certain projects and programmes to the local level, for example youth care initiatives, government is in fact opening up avenues for system developers to control eGovernment (Keymolen & Prins 2011). In central government, it is a knowledgeable organisation such as the ICTU, subject to the administrative supervision of and accountable to the Ministry of the Interior and Kingdom Relations, that is constructing a nation-wide system; in local and regional government, on the other hand, the authorities are forced to contract commercial (or semi-commercial) parties themselves when constructing the local version, with only scant public supervision of the influence that such parties exert on policy. Ultimately, however, these are in fact the systems that create the categories that define the citizen profiles used by government. And if we assume that 'categories have politics', it is important to know where and how the categories have been created.

6.2.4 DECISION-MAKERS

"Instead of vacating it, then, ICT tends to fill the 'seat of power' – in both the literal and metaphorical senses – with even more occupants" (Van de Donk 1997: 502). And among those occupying that seat are a growing number of 'decision-makers', i.e. organisations, foundations and agencies that take many of the crucial policy decisions in the development process – indeed some are set up specifically for that purpose – without, however, being subject to much direct (democratic) supervision. Examples include the EKD.NL foundation (for the Electronic Child Dossier – Keymolen & Prins 2011), Nictiz (for the Electronic Patient Dossier – Keizer 2011; Pluut 2010), and the Personal Records Database and Travel Documents Agency (BPR), which has played a key role in designing the Dutch biometric passport and communicating about its development (Böhre 2010; Snijder 2010). The history of the EU Regulation relating to the biometric passport shows that the biometric standards and other important milestones were decided on in unexpected working groups (in this case the Visa Working Party), that *every single one* of the European Parliament's objections was ignored, and that the proposal was ultimately voted through by the General Affairs and External Relations Council. In other words, it was not the Ministers of Justice and Home Affairs who negotiated the draft, but the Ministers of Foreign Affairs who transformed the proposal into a European regulation (Broeders 2011; see Aus 2008 for a detailed description of the procedure). Decisions on technology, standards and data exchange are frequently taken far out of earshot of Dutch citizens and their elected representatives – decisions that influence the technology ultimately used and the information shared between public authorities. The decision by the ICAO to base the biometric passport on face recognition and fingerprinting and the consequent agreements were the result of old-fashioned power politics by a few large countries within the frameworks of the G8, the informal European Group of Five, various EU working parties, and the ICAO itself (Aus 2008). eCall was designed by the eCall Driving Group, an ad hoc committee of 144 participating organisations, most of which are active in the commercial sector (eCall Driving Group 2005). The European Commission is expected to base the relevant legislation on this group's results (Potters & De Vreeze 2010).

6.3 RESPONSIBILITY FOR THE ICT MARKET

The third and final line that defines the interaction between government and the ICT market relates to government's responsibility for what happens in that market. It should be noted that the ICT market is much broader than the world of the system builders and developers. It also encompasses large information-based corporations that build their business models on the personal data of European citizens, but also telecoms and ISPs that no longer treat all data network traffic equally, and instead discriminate (in rates, exclusiveness or transmission speed)

between certain services and applications (disregarding the principle of network neutrality). The public authorities appear to take this responsibility seriously; witness, for example, the decision by the US Federal Communications Commission (FCC) to pass a network neutrality order[22] and the announcement by Commissioner Neelie Kroes that the EU would be tightening its supervision of social networking sites and the privacy settings used there, especially for minors (Kroes 2010). In the past the European Commission criticised the monopoly position of software developer Microsoft; now, it is turning its attention to information giants such as Google and Facebook.[23] The gist of these interventions is that the citizen must be protected against an aggressive and competitive information market. The view expressed by the Dutch Ministry of Justice on the use of biometrics in the private sector is a good example of the sort of discussion that has arisen relating to government responsibility: "In keeping with its duty to protect the interests of the citizen and of society, government can oblige the private sector to follow its example by forcing it to take the same factors into account that the public authorities consider when applying biometrics in the public sector" (Ministerie van Justitie 2010: 33). Various interviewees commented that it is precisely in the area of identity management that government has a role to play. These observations reflect citizens' worries about the way the private sector uses identification tools. The survey conducted at the request of the ECP-EPN and the WRR reveals that the public had deep misgivings about using the use of the BSN and biometrics in transactions (Attema & De Nood 2010: 2). One argument was the risk of fraud. The public are also very uncomfortable with the idea of medical insurers making use of the BSN. Opinions remain sharply divided when it comes to the banks using this identification number (Attema & De Nood 2010: 2). Other surveys have also revealed the public's concerns about the risks associated with digitization, for example financial fraud on the Internet and identity theft (Van Deursen & Van Dijk 2010: 63).

Government may also intervene if the price it is itself paying is too high, for example the cost of investigating identity fraud cases.[24] In addition, government is both in a position to tackle technological security breaches and responsible for doing so. It is no more able than commercial parties to make identity systems and keys entirely secure, but, unlike the market, it does have the authority to take binding decisions relating to security breaches. In other words, government can stipulate who is to bear the burden of certain risks. It can apportion the costs and distribute what Van Eeten (2011) calls the benefits of *in*security and allocate responsibilities to the relevant actors along those lines (Van Eeten 2011). Citizens then have somewhere to turn when problems arise owing to security breaches in identity systems.

Finally, government may need to intervene more forcefully in the ICT market if the effects of using ICT in the private sector spill over into the public domain. Digital identity authentication is a case in point. There are currently almost no

rules or regulations governing the use and quality of digital identities in the private sector; it has even largely escaped political notice. Swimming pools, supermarkets, employers and computer manufacturers are at liberty to experiment with new types of biometric authentication. The quality of these applications, and how that quality is guaranteed, remains unclear, however. Experience has shown that when it comes to digital identities, the boundaries between the public and private sectors are becoming blurred (Van de Hof et al. 2009). In the view of various interviewees, that could undermine the quality of identity authentication in the public sector as well.

6.4 CONCLUSION

Government is an important consumer of ICT products. Conversely, ICT is becoming a key policymaking tool, turning those who develop ICT products into indispensable designers and making government commissioning practices a pivotal issue in the evolution of eGovernment. It is in part within the context of eGovernment commissioning practices that the driving, underpinning and process-based principles must be brought into balance. What this shows, however, is that government often does not have the differentiated knowledge and expertise to develop applications and links itself, making it difficult to inject critical thinking into its expectations of ICT and what it can accomplish. There also seems to be little awareness that commissioning bodies need to be realistic about the merits of the driving principles. Government lacks people who are able to maintain a sense of administrative responsibility when faced with a cornucopia of technical options and their advocates. There is too little that connects commissioning practices to the underpinning principles, for example because no one has a clear idea of how built-in technological standards (Privacy Enhancing Technologies) relate to standards laid down in the law or by society. There are also gaps in the process-based quality of government's commissioning practices, in particular a lack of professionalism and the fact that end users of applications have only limited input into the development process.

In the midst of all the 'administrative bustle' of institutions that are preparing the groundwork for the ongoing development of eGovernment, the tenor of the policy discourse relating to the ICT market and the use of ICT in the social arena is, notably enough, almost entirely one of facilitation. The ICT industry must be facilitated because it is an economic powerhouse, makes a major contribution to GDP and employment, and even, perhaps, because it can easily outsource its activities to a distant country. Government must equip itself with the best possible technical facilities, which it purchases in the ICT market. And the citizen must be facilitated in order to increase his or her productivity. As important as these matters may be, it is also important for politicians and policymakers to pay more consistent attention to government's responsibility for trends and developments in the

ICT market and their impact on society – something that they have failed to do. The unregulated use of biometric identity authentication systems by private organisations illustrates this policy gap.

NOTES

1 RTL Nederland is a commercial TV and radio broadcasting organisation.

2 Nictiz is the National IT Institute for Healthcare in the Netherlands, the national coordination point and knowledge centre for IT and innovation in the healthcare sector (www.nictiz.nl/page/Home/English).

3 http://regelingen.agentschapnl.nl/content/ict-impuls.

4 Interview with H.Wesseling (TNT Post), H. Grevelman (Swiss Life), P. Hagedoorn (3align Information Governance), F. Krom (ING), T. Mekel (Athlon Car Lease), January 2009.

5 Interview with Peter Wijntje and Sjoerd Peereboom (Ministry of Finance/Tax and Customs Administration), September 2010.

6 *De Volkskrant*, 15 September 2010. However, the fact that a French company develops the Dutch passport is a logical consequence of the privatisation of Sdu, which was decided years before.

7 The AIVD is the Netherlands' General Intelligence and Security Service.

8 http://investor.google.com/earnings/2010/Q1_google_earnings.html.

9 http://webwereld.nl/nieuws/65143/rijks-ict-blijkt-walhalla-voor-huurlingen.html.

10 www.ictu.nl/index.php?option=com_content&task=view&id=684&Itemid=26; accessed 2010.

11 Interviews with E. Bogerman (ICTU), January 2010; A. Thijssen and T. Timmermans (Services, Regulatory Burden and Information Policy unit, Ministry of the Interior and Kingdom Relations), October 2010.

12 *Computable*, 6 September 2010.

13 See, for example, the Netherlands Court of Audit on the C2000 system (2003), the P-Direct system for personnel administration (2007b), the rent and care allowance ICT project (2008b) and the lessons learned in large-scale ICT projects (2007b and 2008b).

14 Interview with W. van Vemde (Chief of Police, Gooi- en Vechtstreek Region) November 2010; interview with A. Thijssen and T. Timmermans (Services, Regulatory Burden and Information Policy unit, Ministry of the Interior and Kingdom Relations), October 2010; interview with S. Borgers (CIO for the Ministry of Housing, Spatial Planning and Environment), December 2009. See also Actal 2010.

15 That is according to Monica Gariup, Research Officer at Frontex (EU Border Management Agency) during a conference in Brussels on the planned European Entry/Exit system (4 November 2009).

16 F. Paul, responsible for the large European migration databases within the European Commission, paints the same picture (interviewed in January 2009), as does P. Hustinx, the European Data Protection Supervisor (interviewed in March 2010).

17 Interview with Peter Wijntje and Sjoerd Peereboom (Ministry of Finance/Tax and Customs Administration), September 2010.

18 Raised, for example, in the interview with T. Timmermans and A. Thijssen, October 2010, Timmermans (Services, Regulatory Burden and Information Policy unit of the Ministry of the Interior and Kingdom Relations, and S. Borgers, CIO for the Ministry of Housing, Spatial Planning and Environment.

19 "The name Logius is derived from the word logical. It refers to the way in which GBO.Overheid's products and services are interrelated, and that they make connections possible," according to the website (translation).

20 Interview with A. Thijssen and T. Timmermans (Services, Regulatory Burden and Information Policy unit, Ministry of the Interior and Kingdom Relations), October 2010.

21 Interview with N. Kaptein, CapGemini, June 2009.

22 www.fcc.gov/Daily_Releases/Daily_Business/2010/db1221/DOC-303745A1.doc

23 www.fcc.gov/Daily_Releases/Daily_Business/2010/db1221/DOC-303745A1.doc

24 Interview with J. Stam, Ministry of Justice, May 2010.

7 SUPERVISORS OF eGOVERNMENT

We have already discussed many of the 'supervisors' of eGovernment in previous chapters. They are bodies charged with reviewing the ICT-related aspects of the relationship between government and the citizen, forcing changes where necessary, and/or urging such changes. This chapter looks more closely at the responsibility that these organisations bear in relation to government's digitization projects and programmes. Our main focus, however, will be on how they perceive their role and how they actually fulfil it. Various actors have been assigned, and in fact play, a role as critical observers of eGovernment, making them vital to the necessary system of checks and balances. In recent years, the Council of State, the Data Protection Authority, the Office of the National Ombudsman, the Netherlands Court of Audit, and – to a lesser extent – the judiciary have all developed into more or less critical 'supervisors' of government's ICT policy aims. They influence the design and ongoing development of eGovernment and the direction that it takes, all within the context of their own responsibilities and with their own set of tools. Yet another, exceptional, supervisor is 'the citizen', who monitors the development of eGovernment in many different ways. Technology has also dramatically altered the nature of such supervision in recent years. There are definite assumptions in eGovernment relating to the role of citizens: what they need to be vigilant about, how much vigilance is required, what they can object to, and how.

7.1 EXISTING SUPERVISORY BODIES

7.1.1 COUNCIL OF STATE

The Council of State advises on legislation and as an advisory body, it also evaluates the construction of eGovernment. In addition to analysing the legal substance of legislation proposing the use of technology or information for a particular purpose, the Council of State also analyses the policy-related aspects and assesses the quality of the proposed legislation on technical grounds, i.e. as a piece of legislation. Because the Government is not obliged to follow its advice, however, the Council of State must ultimately depend on those to whom it addresses its recommendations, the quality of their responses and – if its advice is rejected – whether the Government's arguments in fact hold water (Raad van State 2010: 127). The Council often assesses the legal and technical quality of bills relating to ICT with a view to the fundamental rights involved, the European Convention on Human Rights and the Dutch Personal Data Protection Act (*Wet bescherming persoonsgegevens*, WBP). It was within the context of such an assessment that the Council asked the Government to explain more convincingly the necessity and proportionality of processing certain personal data on almost three million medically

insured people as part of a bill relating to allowances for the chronically ill and disabled (Raad van State 2009: 111). Based on its policy-related analysis of a road-pricing bill, the Council of State criticised government's 'techno-trust' in the recording and payment system that the Government had envisaged. Under the provisions of the bill, motorists would be unable to object to the number of kilometres recorded by the 'electronic box'. The Council of State indicated that it did not share the Government's confidence in technology (Raad van State 2010: 159).

In general, then, the Council of State has repeatedly criticised the Government's plans to introduce legislation relating to the deployment of ICT. According to the Council's Annual Report for 2008 (Raad van State 2009: 97), it is not always clear at the time that the relevant bills are submitted to the Council of State for review why the data processing proposed by the Government is necessary. Nevertheless, the Council sometimes has difficulty analysing, identifying and, as a result, assessing all the ramifications and anticipating the effects of such complex problems. Its members have indicated in an interview that, with hindsight, they felt they had not been critical enough about the use of biometrics in passports.[1] The Council of State is also limited by the tools at its disposal for both its technical assessment and policy-related analysis. It must adhere to the applicable statutory regime that provides the framework for its assessment (in the case of many ICT-related initiatives, that is the Personal Data Protection Act) and the individual policy context of the bill. That means that it is almost impossible for the Council, when evaluating the matter, to foresee and scrutinise the broader context in which the system is to function, for example future connections with other applications that result in new information flows.

7.1.2 DATA PROTECTION AUTHORITY

The Data Protection Authority, which oversees the lawful use of personal data, has many different duties. It advises on legislation, deals with complaints, conducts official enquiries, mediates in disputes relating to data inspection and correction, and imposes sanctions. In accordance with the European Privacy Directive, the Data Protection Authority cooperates with supervisory bodies in other Member States and participates in the Article 29 Working Party, which advises the European Commission on privacy law. The limited capacity and resources available to the Data Protection Authority force it to be selective. Right now, it has therefore prioritised its advisory task within the context of proposed legislation and its enforcement task. These choices, and the fact that the Authority combines a variety of functions within a single organisation, have been the object of criticism from several quarters (see Zwenne et al. 2010). It is considered odd that organisations subject to external supervision "… must turn for information and advice to the same official body that may later rap them over the knuckles with

the very information previously provided for advisory purposes" (Brouwer-Korf Committee 2009). The Brouwer-Korf Committee therefore recommended that the supervisory body should not concern itself with advising, providing information or facilitating. The response of the Data Protection Authority was critical in tone: it believes that advising on legislation can and should go hand-in-hand with supervisory work (CBP 2010c).

Regarding the first of the two prioritised responsibilities, advising on legislation, the Authority observes that the number of advisory reports issued in recent years has remained more or less constant (CBP 2010c: 57). A review of its various annual reports shows that the number varies between 38 (in both 2009 and 2010a) and 47 (2008). What is striking about the various pieces of ICT-related legislation is that although the Data Protection Authority became explicitly involved when the bill was being drafted, it often disappeared from view during the legislative process itself. That is odd, considering that later amendments to such bills can have a clear impact on the way personal data is used. A case in point is the ethnicity criterion in the Reference Index for Juveniles at Risk, included after a motion requesting it was adopted by the House of Representatives: the relevant Minister informed Parliament that the Data Protection Authority did not need to be consulted on the matter (Prins 2010b). Also noteworthy is the State Secretary for the Interior's response when asked by Parliament why the amended biometric passport bill had not been resubmitted to the Data Protection Authority.

"That is because we thought that we had taken the Authority's criticisms on board. We have provided further substantiation … We have made our assessment of the interests involved clear. I have even provided a more detailed explanation. I think our assessment is a good one. The Senate must judge for itself, but we have really paid serious attention to what the Authority has said. So I don't consider it necessary to resubmit the bill to the advisory body. We don't do that with the Council of State either. We write a detailed report for the Senate to judge. We agreed on this procedure because otherwise we would be spending all our time consulting advisory bodies. I don't think that's really what was intended …" (Eerste Kamer 2008-2009b; Böhre 2010: 81).

The Data Protection Authority had previously criticised the same bill on fundamental grounds, and had asked the Government to analyse the advantages and disadvantages of a national travel document records system. The Government had responded by adding a few comments to the explanatory memorandum accompanying the bill, primarily by listing the advantages and disadvantages of such a system. However, it devoted only a single page of the memorandum to the Authority's fundamental objections (function creep, risk of abuse, improper and unanticipated use) and did not mention the other objections (relating to inherent technical and security risks) at all. The State Secretary did acknowledge, however,

that "fingerprints and photographs stored in a database that are related to a stolen identity document … could cause the true owner of that identity endless serious problems. Biometric data is not by definition secret and can leave a trail in its wake that permits that data to be gathered without the owner being aware of it" (Tweede Kamer 2007-2008a: 23).

The Data Protection Authority's second core responsibility is enforcement, and it is within that context that it recently investigated the security of hospital data systems, storage by public transport companies of entry and exit data for students travelling on a public transport chip card, and the use of automatic number plate recognition (ANPR). It is difficult to say whether enforcement by the Data Protection Authority is effective, as there has been no research on the matter. What is clear, however, is that such enforcement sometimes causes the relevant Minister to announce new legislation permitting the very activity against which the Authority has taken action. That is what happened in early 2010 when the Authority concluded that storing irrelevant ANPR data was contrary to law. Just days later, the Minister of the Interior and Kingdom Relations and the Minister of Justice together announced plans for a statutory framework that would legitimise such storage (Tweede Kamer 2009-2010f).

There are also other signs that effective enforcement is far from easy for the Authority. For example, it does not always appear to have a very clear idea of the many different applications being developed at local and regional level. As a result, it almost never takes action at that level, if at all, allowing local administrators to pursue their aims seemingly without obstacles, instructions or supervision (Keymolen & Prins 2011). In addition, as explained above, it is precisely at the operational level that data processes transcend boundaries between sectors, but the Data Protection Authority still examines opportunities and risks on a sector-by-sector basis. In its self-evaluation in 2004, it commented that this approach was compatible with the nature and function of supervision (CBP 2004). The two roles that the Authority has prioritised – enforcement and advising on legislation – are sometimes also subject to a particular political dynamic over which the Authority itself has no control. A case in point is the history of the Electronic Patient Dossier. The Minister of Health made strategic use of the Authority's highly critical report on hospital data systems. The problems that it identified in local systems gave the Minister an additional reason to stress the importance of the national EPD system (Eerste Kamer 2009-2010c). Because it did not contradict the Minister's argument (or was unable to do so), it seemed as if the Authority implicitly supported the EPD, or at least preferred a national system to a regional one. What is problematical in this case is that the Authority's findings relating to the security of hospital data systems have not been published, making it impossible to compare them to the security guarantees that the national system was supposed to provide.

The emphasis on enforcement and advising on legislation leaves no room for tailor-made advice, and the Authority has shifted the emphasis from *ex ante* supervision to *ex post* supervision (CBP 2010c: 36). Although people can submit complaints to www.mijnprivacy.nl (a rather static website), the Authority will not deal with individual cases. Neither can private or public-sector organisations use the website to request advice. The Authority does not interact with individual data-processors or citizens, for example in the form of user or advisory boards or consultation rounds, despite being urged to do so (Civil Service Committee on Regulatory Matters II 2004: 15-16). By contrast, the United Kingdom's data protection authority does consult with individual parties in this way (Information Commissioner's Office 2007).

7.1.3 OFFICE OF THE NATIONAL OMBUDSMAN

The Office of the National Ombudsman also monitors the development of eGovernment. It does so by assessing the appropriateness of action taken by government, either on its own initiative or in response to a complaint. According to the method used by the National Ombudsman, appropriateness should be judged according to the criteria of fundamental rights, the appropriateness of the action in terms of legal substance (proportionality, equality and legal certainty), its formal appropriateness (reasons given, fair play) and the standards of due care applied (professionalism, provision of information, administrative accuracy). It is not compulsory for an administrative body to act on the National Ombudsman's assessment.

Unlike the Data Protection Authority, the Office of the National Ombudsman will consider individual complaints by private citizens. Its various annual reports show that it has dealt with a wide variety of complaints about cases of identity fraud occurring in police and other government systems that have attracted widespread media attention; data processing in the systems maintained by the Immigration and Naturalisation Service; the public transport chip card for students (where it turned out that the IB Group, which is responsible for student grants and loans, had handed over the power to resolve problems itself to the public transport companies); photographs posted on a police website of an individual wrongly suspected of a crime; coordination problems between the Tax and Customs Administration, the Social Insurance Bank, various pension funds, and the Social Security Agency related to the operational tasks of the Health Care Insurance Board; and so forth (Office of the National Ombudsman 2009). While these problems cover a very broad spectrum, they are presented in the National Ombudsman's annual reports primarily on an organisation-by-organisation basis. Although the National Ombudsman has emphasised problems arising from the digital supply chain approach in recent annual reports, it is almost impossible to deduce the scale, seriousness and nature of the complaints relating directly to the

use of ICT. In general, it is far from easy to identity such problems in the dossiers compiled over time not only by the Office of the National Ombudsman, but also by the Data Protection Authority and, more recently, by the Identity Fraud Helpdesk. Indeed, these organisations themselves do not have a very clear idea. In their analysis, Choenni et al. (2011) show that the records held by all these organisations are difficult, if not impossible, to relate to the role that ICT has played in the complaints they have received. In addition, the Data Protection Authority has classified many obviously ICT-related complaints in the very general main category of 'Other'.

7.1.4 NETHERLANDS COURT OF AUDIT

The Netherlands Court of Audit investigates whether central government revenue and expenditure are received and spent correctly and whether central government policy is implemented as intended and has the intended effects. As noted in previous chapters, this is an important task in light of the eGovernment 'drive'. After all, the Court of Audit checks whether the intended improvements in policy effectiveness and efficiency have actually been achieved. It is up to the Government and/or Parliament to attach consequences to the Court's conclusions and to judge them in political terms.

As already pointed out in previous chapters, the Netherlands Court of Audit has been critical – sometimes highly critical – of both government's ICT projects and its approach to information management. Although it is reasonably easy to investigate the revenue and expenditure involved in ICT projects (the incoming and outgoings are relatively easy to quantify), that is otherwise when it comes to assessing government's information management systems. The Court has nevertheless long been critical of government in this area as well. It believes that government does not pay sufficient attention to information management, and explains this by pointing to the fact that in government, "information management 'merely' supports the operational process, unlike in commercial enterprises" (Netherlands Court of Audit 2009: 8). Sustainable information management, however, is "very unlikely to develop without the ongoing attention and perseverance of the Ministries' senior officials and political leadership" (Netherlands Court of Audit 2009: 8). Problems are now too often depicted as incidents and resolved by taking ad hoc measures, until the next problem arises and has to be tackled. In the Court's view, government should develop a strategic agenda for dealing with the rapid changes brought about by the digitization of information. It should, for example, be considering how to archive digital information in the form of e-mails, text messages and tweets. When using a piece of information for the first time, government must already consider how best to archive it and make it retrievable and explore the extent to which it is important for heritage reasons (Netherlands Court of Audit 2010b). The Court also comments, however, that its own survey of

information management abroad has not produced any examples of good practices appropriate to the Dutch style of public administration (Netherlands Court of Audit 2009: 21). Incidentally, the Court has repeatedly advised government to develop a strategic agenda and framework for archiving, deleting, and storing digital files (Netherlands Court of Audit 1991; Netherlands Court of Audit 1998), and it is not alone in that respect: the tone struck in two reports by other advisory bodies, one by the Archives Division of the Cultural Heritage Inspectorate (2005) and one by the Council for Culture and the Council for Public Administration (2008), is one of alarm. The Archives Division observes that government organisations frequently have no idea where they have stored their digital operational and accountability information. Senior public administrators should play a much more active role in coordinating and organising information management (Archives Division of the Cultural Heritage Inspectorate 2005). In its various responses, the Government agrees with the conclusions of these reports. It recognises the need to define a strategic agenda, to take a comprehensive approach, and to change the internal culture of public administration (Tweede Kamer 2008-2009e). Not only has there been explosive growth in the quantity of information, but it is also being provided in a rapidly changing succession of different media. Inevitably, any strategic agenda relating to archiving and digital sustainability will lag behind. It is therefore crucial for government to get a grip on the dynamic issue of archiving and digitization. According to the Government, sustainability should be considered at the 'front end' of the information chain, given the importance of operational management, accountability and cultural heritage (Tweede Kamer 2005-2006b: par. 3.2.). The President of the Netherlands Court of Audit, Saskia Stuiveling, said in an interview that there is much more involved than shifting the focus to the front end of the information chain, however. Gradually, it is becoming clear to what extent the digital archive can be 'engineered'. Perhaps we must simply accept that archives tend to grow organically and focus in particular on search strategies. It is important to come up with new ways of retracing information that we once thought we would never need again. Government must work on a cultural transformation with respect to digitized information processes. It must leave behind its traditional linear approach to creation, use, management, and archiving and start regarding these as simultaneous processes in which all information, regardless of its purpose (operational process, institutional memory, cultural heritage, accountability, legal claims, evidence) is considered of equal value and viewed as a coherent whole. This means that the bureaucracy will have to function more as an open system.

7.1.5 JUDICIARY

Whereas policymakers are under no official obligation to heed the advice of the bodies referred to above, they ultimately do have to adhere to rulings by the courts. Nevertheless, the public – who approach the Office of the National

Ombudsmen and even, to a more limited extent, the Data Protection Authority with complaints about government digitization – scarcely ever turn to the judicial authorities. That is also the case in other countries (Mayer-Schönberger 2009: 138-139). It is evidently difficult to 'kick-start' an individual to initiate court proceedings on a matter of information: citizens are handed decisions that are unfavourable to them but are unaware that their case can also be viewed as a dispute about the underlying information. For example, various reports evaluating the Personal Data Protection Act have noted that judicial rulings related to the Act have been very few in number (Zwenne et al. 2007; Winter et al. 2008). This observation can be applied to other legislation governing the way personal data is dealt with, for example the Police Data Act (*Wet politiegegevens*), the Municipal Database (Personal Records) Act (*Wet GBA*), and so on. In short, the courts have had little opportunity to interpret and enforce rules pertaining to the digitized processing of personal data. Rare exceptions include the ruling by the Court of Appeal in Leeuwarden (June 2010),[2] which concluded that there was no statutory basis for using images from motorway cameras in a criminal investigation, and the ruling by the Dutch Supreme Court (March 2010) on a case in which the Public Prosecutions Service had demanded data from Trans Link Systems (Buruma 2011). The Public Prosecutions Service had requisitioned name and address details and ID photographs of all passengers travelling on a public transport chip card who were present in certain Rotterdam metro stations at a specified time, as part of a criminal investigation. The Supreme Court ruled that the ID photographs could only be requisitioned after authorisation by the delegated judge, and could only be used in a criminal investigation after such authorisation had been obtained.[3]

The picture is somewhat different when people are affected financially. Examples are the various court cases relating to errors in the systems used by the Tax and Customs Administration, or the exchange of data with an external organisation contracted to issue tax demands (Gribnau 2010). The latter was the subject of a court case in 2009. A system error led to incorrect data being exchanged between the municipal personal records database and Cocensus, the firm that the relevant local authority had contracted to issue tax demands in respect of waste material. The local authority had attempted to recover the missing amount from the public later on, but the court ruled that an additional demand was not possible.[4] As in the case of the Data Protection Authority and ANPR, however, the Government is a sore loser at times and, just days after a negative decision by the courts, may announce new legislation changing the situation in its favour. A case in point is the response of the Minister of Finance to the Supreme Court's ruling that, in the event of an erroneous tax demand owing to an error in the design of a computer system, an additional demand would not be possible.[5] The Minister presented a bill that would make additional demands possible in the event of major errors due to the use of ICT (Tweede Kamer 2009-2010h).

The judiciary in the Netherlands has little opportunity to comment on government's ICT aims, especially when compared with other countries. In a memorandum addressed to the Senate, the Minister of Justice suggested that the Netherlands lacked "an organised movement that could claim to represent citizens who are specifically attempting to protect their data", and that the absence of such a movement influenced the number of data-related disputes submitted to the courts (Eerste Kamer 2009-2010a: 48). Potentially even more important is that the Netherlands does not, as yet, have any means of testing the constitutionality of a legislative act. Rulings handed down not only in Germany (for example the ruling of 2 March 2010 on data retention),[6] but also previously in Romania (8 October 2009)[7] show that constitutional courts are sometimes willing to overrule legislation permitting government to use personal data because they consider it a breach of fundamental principles. The international courts – and in particular the European Court of Human Rights – have also been very consistent (De Hert 2011); they have been critical of government's policy objectives and, in a nutshell, have ruled that states must exercise restraint when using technology to gather and use personal data (De Hert 2009).

7.1.6 NEW ARRANGEMENTS

Alongside the Netherlands Court of Audit, the Council of State, the National Ombudsman, the Data Protection Authority and/or the judiciary, there are other actors and government organisations that have been designated or have taken on a regulatory, supervisory and accountability role in recent years. For example, the CIOs described earlier provide Parliament with timely, accurate information in order to support its supervisory powers. In the Coalition Agreement, the Rutte Government has agreed to institute a national supervisory body for data leaks: "The government will produce proposals for all public and private-sector information society services to have a duty to report any loss, theft or abuse of personal data to a national supervising body, which will have powers to impose fines if any leakage of such data is found not to have been reported" (official translation of Regeerakkoord 2010). The UK had a regulator specifically charged with supervising identity management issues, i.e. the Identity Commissioner. However, the Cameron Government, which took office in May 2010, scrapped the Identity Cards Act of 2006 and with it the office of the Identity Commissioner.

In addition to new institutions, there are also new arrangements, specifically those made between the various agencies, which have set up their own systems of checks and balances. This is in fact a much older development, but the use of ICT has clearly been a stimulating factor. The new arrangements have their origins not only in the tools that have emerged with the rise of technology, but also in the need to respond to the specific complexity involved in using ICT and the changes that it effects in relationships. One example relates to the client councils and

customer panels set up by the Social Insurance Bank and the Social Security Agency to enable citizens to discuss and provide feedback on online initiatives (such as the Digital Insurance Report or on www.burgerpolis.nl). Other initiatives – for example the gateway review and IT Dashboard – provide Parliament with more up-to-date reports on the progress of ICT projects, in particular large-scale ones (Snijders 2011). Online complaints desks such as the Identity Fraud Helpdesk and the Citizen Service Number Helpdesk also illustrate the new supervision and control arrangements. According to the National Ombudsman, Alex Brenninkmeijer, it is precisely the human factor that makes some of the above-mentioned arrangements a success. The quality and integrity of systems depend in large measure on the way human feedback and feedback loops are organised, for example through the 'Stella teams' set up by the Tax and Customs Administration.[8]

One increasingly popular tool consists of Privacy Enhancing Technologies (PETs). In effect, this tool integrates supervision and enforcement of the statutory rules for dealing with personal data into the technology itself. Remarkably, Parliament had already called on the Government to apply PETs in its systems on 18 November 1999, when it voted overwhelmingly in favour of a motion to that effect submitted by MP Atzo Nicolaï (Liberal Party/VVD) (Tweede Kamer 1999-2000). So far, however, this request has scarcely been followed up. When the Ministry of the Interior and Kingdom Relations asked seven government organisations to set up trial projects in 2003, they responded that it was not an opportune time to start working with PETs (Borking 2010). The same year, a study commissioned by the same Ministry and carried out by RAND Corporation Europe listed the top five government arguments against PETs: the existing methods of protecting privacy were sufficient; privacy did not need to be protected; experiments with PETs were a threat to the reliability, quality of service, and image of the government body concerned; PETs were not a mature technology; and there was not enough time, money or man-power available to introduce PETs (Borking, 2010). Three years later, the evaluation of the Personal Data Protection Act determined that that attitude had not really changed (Zwenne et al. 2007). Today, however, the climate seems more favourable: there are now loud calls to take PETs seriously, both at the international level (the European Commission's Article 29 Data Protection Working Party and the European Data Protection Authority) and in the Netherlands (the Government, Parliament, and the Dutch Data Protection Authority).

7.2 THE MULTIFACETED CITIZEN

More broadly speaking, there are naturally also supervisory entities operating outside the context of government. The role of the media springs to mind, whose coverage and criticism of eGovernment has been mentioned numerous times in this book. A growing number of citizen initiatives and citizen and consumer

representatives have set themselves up as irritants and regularly force government to account for its plans and aims or to modify them. In response to the action group 'we don't trust voting computers' (*wij vertrouwen stemcomputers niet*) the Dutch cabinet in 2007 even decided to take voting computers out of service. In some cases, citizens mobilise and form official, professional organisations, for example the Dutch Consumers Association; in other cases, they set up flexible, ad hoc groups. The way in which such groups and organisations themselves use ICT has dramatically changed the 'mobilisation of public opinion'. The lightning speed at which information can be disseminated through ICT and the social networking media can nip a policy proposal in the bud, raise it for discussion (for example the vaccination for cervical cancer), or tip the political debate one way or another (as the account below of the biometric passport will show). Citizens have a different attitude toward government than they used to, one that appears to encourage ever-greater activism when it comes to government's use of ICT. Activist-citizens want to do more than simply monitor government, and they often operate very differently to the 'traditional' supervisory bodies. Although such grassroots campaigns are often intended to supervise and correct, some go a step further. Aided by social networking media, dissatisfied citizens take over government responsibilities themselves or take action to make government more transparent (and therefore easier to scrutinise). Nevertheless, it remains difficult for individual citizens to 'take part' in the process and 'contribute' to digitization initiatives. For example, it is rare for government to set up a public consultation process while preparing new policy and invite the public to comment.

7.2.1 INFLUENCING POLICY

One good example of how the citizen can influence policy is the bill introducing the smart energy meter, which was rejected by the Senate in April 2009. After the Consumers Association had let the Senate know its objections to the bill, sharply criticising its privacy implications (Eerste Kamer 2008-2009a), and after citizens had campaigned against it, for example on the website *www.wijvertrouwen slimmemetersniet.nl* ('www.wedonottrustsmartmeter.nl'), the Minister was compelled to amend the bill. In the new version, the data generated by the energy meter could only be used with the end user's consent, the only exception being some basic information required for invoicing purposes (Tweede Kamer 2009-2010e). In the original bill, the end user had no say in how the data would be used.

7.2.2 TAKING CONTROL

Citizens do not always campaign because they want to see changes in policy. Their dissatisfaction may also lead them to take over government's traditional tasks themselves. A well-known and controversial example of 'citizens' justice' is the website *www.stopkindersexnu.nl* ('www.stopsexwithchildrennow.nl') and its

successors, with each new website being launched when government takes steps against the existing one. The websites publish the whereabouts of convicted paedophiles who have been rehabilitated. The parents who produce, consume and act in accordance with this application in a variety of ways do indeed have every interest in knowing that a convicted paedophile is moving into their neighbourhood, but the 'ad hoc justice' that it advocates undermines the principle, upheld by the law and by government, that every offender must be allowed to reintegrate into society. Another, more playful, attempt to undermine government enforcement of the law is the website www.flitsservice.nl ('www.speedcameraservice.nl'), which continuously updates the locations of stationary and mobile speed cameras (for example those built into waste disposal bins).

7.2.3 MORE TRANSPARENCY

Besides campaigns aimed at changing policy or at taking over government tasks, citizens can also agitate for more government transparency. For example, organisations such as The New Way of Voting Foundation (*Stichting Het Nieuwe Stemmen*) and others advocate transparency and public participation via the Internet, whether they are aiming to encourage more informed voting on the part of citizens (www.wiekiesjij.nl; 'www.whowillyouvotefor.nl'), to boost the right of citizens to petition government and take the initiative themselves (www.petities.nl; 'www.petitions.nl') or to lower the threshold to approaching politicians (www.maildepolitiek.nl; 'www.emailpoliticians.nl'). Another example is the Critical IT Infrastructure Foundation (*Stichting Kritische IT Infrastructuur*), which hopes to launch a fundamental discussion of the political, social and administrative considerations involved when the public sector selects systems, software and ICT suppliers. A more institutionalised countervailing power emanates from the Government Information (Public Access) Act (WOB), whose impact was recently boosted by a tool that encourages and enables ordinary citizens (as opposed to journalists) to submit requests for information under the terms of the Act (www.woberator.nl). Although government today discloses far more information than it ever did in the past, its brand of transparency only produces information products that have already been 'processed': reality has already been converted into information (for example on policy). More radical are the 'open data' initiatives such as those in the United Kingdom, which the Netherlands is cautiously beginning to emulate.[9] These provide raw government data, rather than government information, so that the citizen can actually study the choices that government makes based on the data available to it. Citizens can also give their creativity free rein with such data and come up with new applications for it, such as pollution maps, crime maps (which combine police bulletins with designated locations) or the BBC News map (a map showing the locations of news stories reported by the BBC).

The influence of these various citizen initiatives is evident in the extent to which government embraces them and takes them on board. Government is increasingly supporting and/or adopting such initiatives. For example, both the Citizen Link (*Burgerlink*) programme run by the Ministry of the Interior and Kingdom Relations and the website *www.digitalepioniers.nl* ('www.digitalpioneers.nl') have been set up by government to endorse and support citizen initiatives. A government endorsement may create a difficult dilemma for the initiators, however: they must choose between accepting funding and thereby losing their autonomy or continuing independently without any financial support, fuelled only by their enthusiasm.

7.2.4 CITIZENS AND THEIR GUIDING PRINCIPLES

Citizen initiatives are becoming something more than a countervailing power operating in the margins. Grassroots movements collaborate with well-known international human rights organisations, rapidly mobilise followers through the new media, have access to substantial financial resources, and step into the arena well-armed with expert advice, for example from lawyers. Resistance against the biometric passport gained momentum in the summer of 2009, when a broad coalition of NGOs headed by the Netherlands Committee of Jurists for Human Rights (NJCM, the Dutch section of the International Commission of Jurists) instituted proceedings before the United Nations Human Rights Committee against the Government's plans under the new Passport Act to store all biometric passport data in a national database.[10] The digital citizens' rights movement Bits of Freedom was subsequently revived and organisations such as the Dutch Consumers Association also became involved in the privacy debate. The discussion was gradually taken over by professionals, with a possible entrenchment of positions as a result. In 2009, the Privacy First Foundation began, with the assistance of a law firm, to prepare a case against the Minister responsible for the Passport Act. The Vrijbit ('Freebit') association had already attempted to block the new legislation by instituting emergency proceedings before the European Court of Human Rights. In late November 2009, another organisation (Het Nieuwe Rijk, i.e. 'The New State') distributed a leaflet designed to resemble a government leaflet and calling on citizens to have their Citizen Service Number tattooed on their arm. The relevant State Secretary announced that the Government would take legal steps against this campaign. On 11 January 2010, the Public Prosecutions Service let it be known that it would not consider the State Secretary's complaint. A day later, however, the Dutch Advertising Code Authority claimed competence in the matter and judged that the 'advertisement' was contrary to the Dutch Advertising Code.[11]

Although society tends to be most critical when the underpinning principle of privacy is at stake – as shown in numerous examples given above – there have also been campaigns for the process-based principle of transparency. For example, the

Critical IT Infrastructure Foundation mentioned above wants ICT systems to be selected for reasons other than operational considerations alone; it would like more consideration to be given to the transparency and democratic supervision of applications and systems and to the autonomy of government. In one sense, citizens who organise themselves into groups of this kind are acting as a new type of supervisory body, and they believe they have a role to play in organising countervailing forces aimed at preventing or undoing certain government ICT initiatives or raising them for discussion. But the rise of such citizen movements and their efforts at supervision and control also raise questions about the tools they use or have available, their legal position, and the legitimacy of their efforts: To what extent do they speak on behalf of citizens? Are the procedures that result in the decision to take action transparent? Are the sources on which they base their efforts sufficiently reliable, known and verifiable?

7.3 CONCLUSION

The consequences of eGovernment are becoming more apparent all the time. Judging by the growing level of activism, this increasing visibility has sparked off a debate on the desirability of eGovernment and the direction that it should take. It is nevertheless a debate that has been defined (so far) by pure chance. In some cases, the dynamic social forces that turn a certain question into a 'hot issue' only erupt long after official decision-making has ended. The example of biometric data in passports shows that political decision-making and accountability may be out of touch with the perceptions and sensitivities of the public. At the same time, however, the attention focused on this particular issue was rather arbitrary: there are numerous other issues requiring public discussion that are simply not getting the attention they deserve. In most cases, it seems that 'society' has left the job of evaluating eGovernment in the hands of Parliament (and the Government) and the 'supervisors' that are indirectly involved. These institutions face the difficult task of deciding, one application and one connection at a time, how best to design the digital relationship between government and the citizen. It is not easy for such 'supervisors' to pinpoint and weigh up the concerns and interests that must be addressed and then reach an opinion on them. In terms of their duties and scope of interest, the existing bodies that supervise eGovernment are either restricted to assessing applications without viewing (or being able to view) them in a wider context, or limited to assessing a particular aspect of the development of eGovernment.

This chapter has considered not only how policy decisions are influenced by the supervisory bodies identified, but also how transparency and accountability are generated for individual citizens. That involves assessing the citizen's position with respect to information (transparency) and the citizen's access to redress (accountability) in cases in which individual interests are affected. There have

been major problems in this respect, as the National Ombudsman has been quick to point out, although – remarkably enough – neither the courts nor the Data Protection Authority have asserted themselves in such cases. Those problems can be summarised as follows. Efforts to develop an efficient but equally client-driven eGovernment have not been accompanied by efforts to give the citizen a better understanding of his or her own information position and the possibility of taking corrective action in that respect. The chains and networks of information that aid government in its tasks have not been counterbalanced by chain-like or network-like protection for citizens. It will be necessary to find that balance, because eGovenment engenders great vulnerabilities in the small number of cases in which information processes go wrong, despite its also offering enormous advantages in the larger number of cases in which information processes function correctly.

NOTES

1 Interview with C.J.M. Schuyt, M. Oosting, M. Raijmakers, H.J.T.M. van Roosmalen, Raad van State, April 2010.

2 LJN: BM8100 (www.rechtspraak.nl).

3 LJN: BK6331, Dutch Supreme Court, 08/04524 B (www.rechtspraak.nl).

4 Haarlem District Court, 11 September 2009, no. 09/902, NTFR 2009/2158.

5 Dutch Supreme Court, 14 March 2008, no. 43.301, NTFR 2008/551.

6 Bundesverfassungsgericht, 2 March 2010, case nos. 1 BvR 256/08, 1 BvR 263/08 and 1 BvR 586/08; see www.bundesverfassungsgericht.de.

7 Curtea Constituţională 8 October 2009, case no. 1.258, www.ccr.ro/decisions/pdf/ro/2009/D1258_09.pdf, consulted on 18 November 2010.

8 Interview with A. Brenninkmeijer, Office of the National Ombudsman, February 2010.

9 See Ministerie van Economische Zaken, Landbouw en Innovatie, 2011.

10 See www.njcm.nl/site/press_releases/show/25; www.binnenlandsbestuur.nl/nieuws/2009/07/protest-tegen-opslagvingerafdruk.121883.lynkx.

11 Decision by the Dutch Advertising Code Authority (*Reclame Code Commissie*), Amsterdam 12 January 2010: www.reclamecode.nl/consument/default.asp?nieuwsID=391&terugURL=%2Farchiefnieuwsberichten%2Easp%3FhID%3D7.

PART III

ANALYSIS AND RECOMMENDATIONS

8 iGOVERNMENT

Modern ICT offers government many tempting opportunities to speed up work processes, increase the effectiveness and efficiency of policy, offer better and more customised services, and lighten the load of bureaucratic paperwork. The aim is to make government streamlined, digital and service-minded while at the same time satisfying the citizen and 'client'. In addition, ICT is increasingly being used in policymaking in the care sector and in the interest of public safety and international security. New systems and their interconnections are meant to make both the community and the world a safer place for the citizen. Indeed, innovative use of the new technology is rapidly becoming a cornerstone of modern government policy in every area of service, care and control. At the same time, the dynamic nature of ICT influences the 'rules of the game', whether that means the rules that apply to the interaction between government and the citizen, between different government organisations, or between government and private parties. Information is exchanged between organisations and crosses the boundaries between the public and private sectors without proper consideration being given to the implications for the citizen and the authorities. More and more often, government bases its dealings with citizens on profiling and the information that it has gathered, leaving those same citizens powerless and empty-handed if the information is incorrect or is incorrectly interpreted. Furthermore, government is often seemingly unwilling or unable to set limits to its own appetite for collecting data: it is more likely to find reasons to gather more information than to curb its own curiosity.

When it comes to new technology and, in particular, the information flows that new technology generates, government has a double responsibility. On the one hand, it must explore new tools, technological innovations and information flows to determine whether they can improve government policy. On the other, it must also prevent any foreseen and unforeseen side effects of the new information tools from harming citizens (Buruma 2011). The deployment of ICT and the associated information flows in policymaking are never without wider consequences. A purely instrumentalist approach to technology is therefore naive at best and harmful at worst. As we saw in Part II, new information flows also create new social and policy-related realities that have repercussions for citizens and for the authorities themselves. Government must therefore find a way to navigate between two contrasting demands: using ICT innovatively in policy and policy implementation, and protecting citizens against the foreseen and unforeseen effects of ICT, in particular complex information flows.

This chapter places the trends analysed in Part II in a new framework and suggests a perspective on a necessary paradigm shift. It begins by recapitulating the most

important features of eGovernment, i.e. the main framework in which government now relates to ICT. Starting from this framework, we then shift our focus to an entirely different perspective on ICT in government, which we refer to here as iGovernment. This new perspective raises pointed and urgent questions for government that have so far not received the attention due to them when viewed from the perspective of eGovernment and its unilateral focus on technology. By zeroing in on the *information* Government, we focus on the information flows rather than the individual technologies and applications, and show that, far from being 'engineered' by politicians and policymakers, iGovernment is in fact 'emerging' in a very real and empirical sense. This raises questions about how iGovernment is to evolve further and about the relationship between the citizen and government within that context.

8.1 eGOVERNMENT

At first, government regarded ICT primarily as a tool for streamlining its own (internal) organisation and processes, in particular with respect to policy implementation. ICT then became all-pervasive under the 'eGovernment' banner, and the emphasis shifted to the 'outside', i.e. to policy aimed at increasing the effectiveness and efficiency of services delivered to citizens and businesses. eGovernment plans and strategic agendas typically present a positive view of technology. ICT is overwhelmingly regarded as a neutral tool that can be used to achieve certain aims. There is little concern for the context in which ICT and eGovernment is being introduced (Bekkers & Homburg 2009: 227), or for the other foreseen and unforeseen effects of using technology (De Mul 2003). Technology is 'rolled out', work processes are 'streamlined', and services are 'updated'. 'Techno-trust' prevails.

It should be noted that there is growing concern regarding the coherence and coordination between the different systems emerging in the back office of government, specifically with respect to service provision. That concern focuses mainly on the technical aspects, however, such as interoperability[1] and open standards, and not on how to keep networked information in check. Neither is there much discussion of the dependencies and vulnerabilities created by the coherence that is sought by the coordination between organisations and interoperability of information. When vulnerabilities are acknowledged, they are resolved by a new form of 'neutralisation': technology itself is put forward to neutralise the risks associated with technology with the help of 'privacy by design'[2] and 'privacy enhancing technologies' (PETs).[3] Because politicians do little more than pay lip service to these new solutions, however, they have not turned out to be the solutions that they might have been. A motion adopted by the House of Representatives in 1999 to apply PETs in new government systems has so far been largely disregarded, despite a recent resurgence of enthusiasm in the House. In addition, the focus on

technology encourages politicians to continue viewing it as a neutral tool; the possibility that a given application involves social change and risk is glossed over in discussions by portraying it as an eminently *practical* innovation. The emphasis on technology also signifies a failure to properly consider what it means for the relationship between government and the citizen to be transformed into a relationship between a service provider and a consumer – a key idea in the thinking behind eGovernment. Highlighting the service aspect of that relationship also makes government vulnerable: it raises expectations among citizens that government certainly cannot always live up to, especially when compared to the ICT-driven services provided by businesses (which are also not always ideal).

Although government White Papers still demonstrate a strong belief and trust in what ICT can achieve, real-life experience in the twenty-first century has enriched the eGovernment discourse and made it somewhat more subtle. The emphasis is still on the opportunities that ICT offers government, but there is also growing concern regarding the barriers that stand in the way of achieving eGovernment, for example the integration and coordination problems that arise when attempting to set up a one-stop helpdesk or integrated provision of electronic services. A growing number of warnings can be found in the academic literature and in advisory reports to government. In 2007, for example, the Postma-Wallage Committee echoed previous reports in noting a lack of coordination and major differences in speed, but also the absence of any sense of urgency.

> "Many of our interviewees see the implementation of eGovernment mainly as a 'technical operation' that has no clear relationship with the substance of policy. We can attribute this to the almost total lack of attention among politicians and policymakers at national and local level. Far too often, the projects have remained the province of technical experts" (Postma-Wallage Committee 2007: 9).

Despite such clear warnings, government's more recent ICT policy documents – including its *ICT Agenda 2008-2011* (Ministerie van EZ 2008) – continue to speak in terms of 'priority topics' without addressing the associated challenges and broader implications.

8.2 FROM eGOVERNMENT TO iGOVERNMENT

If we look beyond the applications and layers of digitization introduced within the context of eGovernment, we find a hodgepodge of information flows running within and between the various authorities, both inside and outside the relationship between the citizen and government. It is extremely rare, however, for government policy to explicitly prioritise information and its management. Step by step, decision by decision, the everyday work of government is giving rise to

'information government' without this being based on any overall strategic agenda or awareness among political decision-makers. Paradoxically, government is constructing iGovernment without being aware of its existence. Because politicians have failed to recognise that government has become iGovernment, the latter has no 'natural' limits – a feature reinforced by the tendencies inherent to the developments described in Part II of this book.

First of all, effectiveness, efficiency and security are manifestly the most important driving forces behind the introduction of technological applications and connections between them. Secondly, the policy domains of service, care and control are becoming increasingly interwoven. Thirdly, personal information is growing more and more important within the various information flows. These tendencies are giving rise to various risks that this book aims to identify. For example, the fact that politicians are seemingly unaware of the rise of iGovernment means that government risks losing its grip on this development. The absence of any proper organisational and institutional framework can also lead to externalities that will require a great deal of time, money and effort from government. Finally, if no proper frameworks are created for iGovernment, the citizen could lose confidence in government – as could government agencies in one another – as a reliable custodian and user of information. Without this confidence, however, iGovernment cannot innovate its primary processes and policy.

8.2.1 CROSSING THE BOUNDARIES OF eGOVERNMENT

Although it is not necessary to immediately discard the eGovernment paradigm as such, iGovernment does not match the overriding image of eGovernment in a number of significant ways. That is because iGovernment differs entirely in its features from eGovernment. Viewed through the lens of iGovernment, it is not individual technical facilities that matter as much as information and information flows.

Public authorities have always had a natural inclination to gather information in order to intervene in society on the basis of that information. Torpey (1998) observes that the state first embraces society in the informational sense before taking effective action. This means gathering as much information as possible, for one thing by means of a finely meshed administrative infrastructure, and then using that information across the full breadth of government policy. According to a study by the Data Protection Authority, the average Dutch person is linked to 250 to 500 different records, with the lower limit being associated with someone who 'lives like a hermit', according to the Chairman of the Data Protection Authority, Jacob Kohnstamm (Schermer & Wagemans 2009). The potential to 'embrace society' has increased dramatically in recent years, and will indeed continue to do so in the foreseeable future. The sharp increase in storage and computing capacity and the growing level of interoperability between different

systems mean that, in the *infrastructural* sense, the facts have overtaken eGovernment. That infrastructure makes a number of policy-related and organisational developments possible that have also radically changed the nature of digital government in the practical sense.

To begin with, technology – as the previous chapters have shown – is no longer deployed merely to improve and streamline government *service* provision but also to gather and link information for *care* and *control* purposes. Increasingly, ICT plays a vital role in youth policy and healthcare (care), and has become indispensable in immigration policy and security policy, both to fight crime for counterterrorism purposes and in the more everyday enforcement of the law (control). With respect to security, information is passed not only between organisations in the Netherlands but also between the Netherlands and other countries and international organisations. The infrastructure of digitization and interoperability make it much easier for information to be pooled in what are essentially separate domains of service, care and control. Thanks to technology, the boundaries between these domains – which were never very sharply defined in the first place – are becoming increasingly blurred.

Secondly, the importance of networks of actors and, in particular, information networks continues to grow. The number of partnership and information arrangements between public and private actors is growing both within and outside government, giving rise to complex reciprocal information interdependencies. Private and public information flows also get blended together into these networks. The authorities are growing increasingly interested in the information gathered by private individuals and enterprises, and they make considerable use of such information. In chain computerisation, information is passed from one organisation in the chain to another; in networks, however, information is exchanged or managed collectively without it being passed along a fixed sequence of actors. Oddly enough, government often refers to chain computerisation rather than network computerisation, whereas in reality it is the latter that is increasingly standard. The dynamic nature of information dissemination and utilisation in networks makes it very difficult at times to decide who is responsible for specific information about citizens (and for safeguarding the accuracy of that information). A network is also a web in which citizens can become entangled, as, for instance, the Kowsoleea case made clear.[4] In the end, even the Office of the National Ombudsman (2009) was unable to track down the complex chain of interactions that led to this case of identity fraud so that the record could be set straight. In eGovernment, government's main problem was how to develop the relevant systems while avoiding the risk of major financial debacles. Today, however, the potential repercussions of faulty information or misdirected information flows represent a different and far greater risk, one that threatens both the individual citizen and government itself.

Thirdly, the growing number of information sources – and in particular the potential for interrelating and processing information – means that iGovernment increasingly makes use of digital profiling techniques, and as a result groups citizens into certain categories. Profiling is playing a growing role in policy and policy implementation. Categorisation of citizens becomes a dominant theme as government applies data mining and other techniques to the information it has stored in order to generate and combine a variety of information sources.[5] To some extent that is unavoidable: the amount of information stored simply exceeds human capacity, forcing government to turn to electronic processing and profiling. What this means in everyday practice, however, is that people are linked to a variety of profiles and 'data doubles', in other words to images put together from various sources of information that then take on a life of their own in the systems maintained by government (and/or business and industry). Such profiles consist of information that is first *de*contextualized – taken out of the context in which it was collected – and then *re*contextualized within the context of the new composite profile. This process is naturally not an exclusively technical affair ('categories have politics'), nor is it without social implications. Such 'images of the future' hinder the autonomy (freedom of choice) of individuals in a way similar to the 'images from the past' that linger so long due to the ICT-revolution. After all, a profile amounts to a prognosis on the future identity of an individual. Government also uses such processes to anticipate the future. Profiles and information processes play a growing role in 'preventive policing' or in the youth care sector, where information gathering and data linkages are regarded as indispensable for preventing the tragedy of child abuse.

Fourthly, trends in the iSociety and trends in iGovernment have an impact on one another. New information-gathering tools are invented outside the context of government. The new social networking media, the behaviour of buyers and shoppers online, and the information collected in the private sector are all generating a potential goldmine of digital trails. That information can be used, within the relevant margins and statutory frameworks, to satisfy government's information needs. At the same time, the mere fact that such information exists only serves to encourage those information needs: there are no natural limits to information gathering, nor are there any restrictions on the extent to which the public and private sectors are allowed to overlap. That too is considered on a case-by-case basis. Citizens place considerable trust in the way government uses their private information – especially when it comes to security matters – but that is no reason not to set limits, especially with the volume of information generated by the iSociety set to grow. On the other hand, government has so far shown little interest in interacting with citizens or even in sharing information with them. Although government espouses transparency and although transparency is also on many a citizen's wish list, in practical terms the authorities never go much beyond good intentions. The potential is there, including in the tools made possible by ICT, but

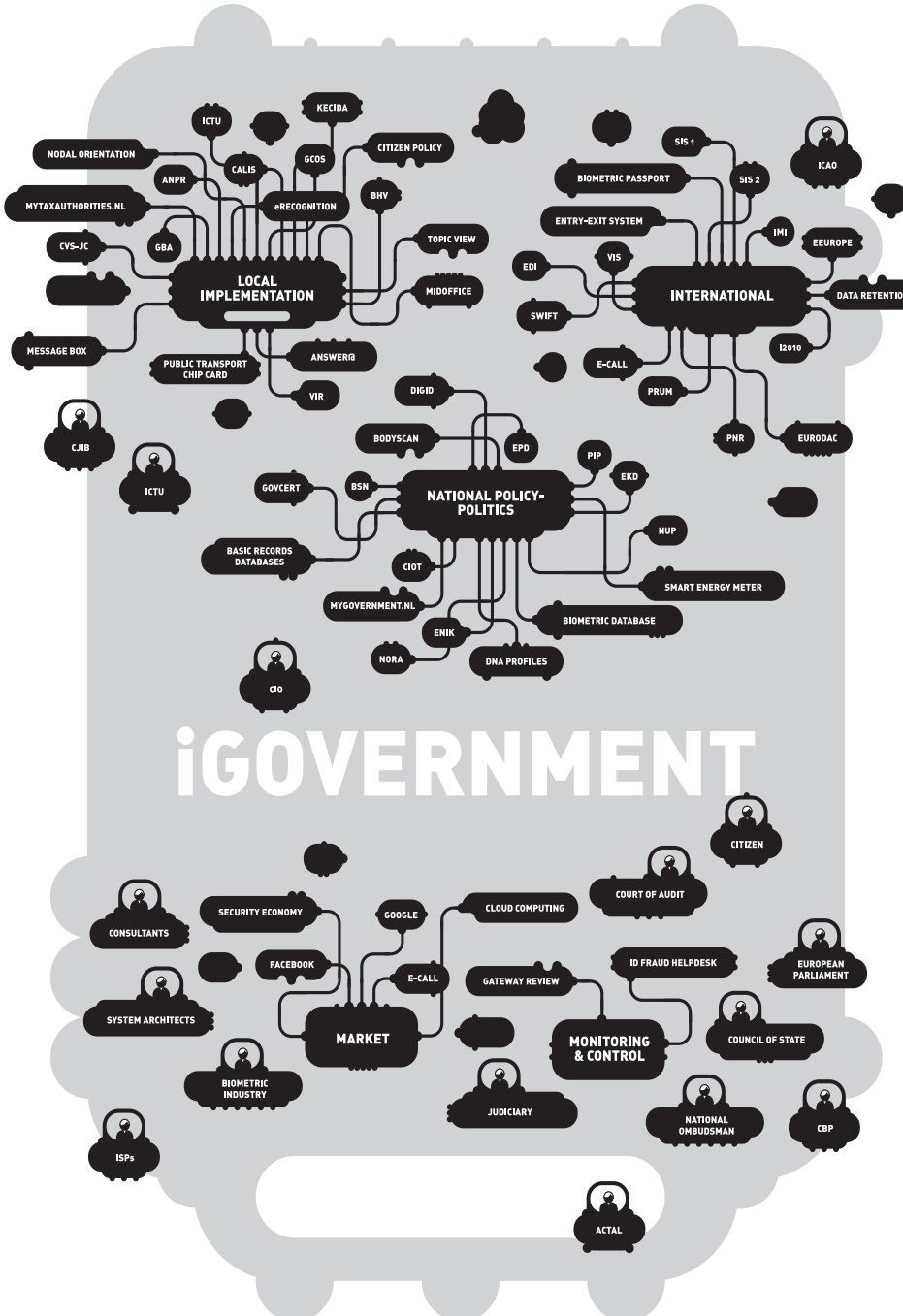
political will and resolve are lacking. As a result, transparency is often a one-way street: the citizen is transparent to government, but not the other way around. The glut of information produced by the iSociety combined with the technology to make it accessible mean that government will have to consider "how well it wants to know its own citizens" but also "how well it wants its citizens to know it".

The traditional focus, contextual frameworks and aims of eGovernment are therefore being overtaken by day-to-day developments. The overlap between service, care and control, the circulation of personal data with in networks, the merging of public and private information flows, and the tendency to use digital profiles to pursue a proactive, forward-looking policy: all these things result from a series of choices relating to individual applications, new systems, and decisions regarding the connections between them. At a higher level of abstraction, the *de facto* result is a network of information flows within the domain of government that has far outstripped the policy and conceptual framework of eGovernment. Critics condemn government's thirst for information and the rapid exchange of data between government services, drawing on images such as 'Big Brother' and the 'surveillance state'. Although change is indeed taking place at a considerable pace, such images are only marginally applicable to the situation that has arisen, mainly because they suggest an intention that is in fact absent: there is no conspiracy or intrigue involved. There is no evil genius designing the 'surveillance state'. And at the same time, that is almost exactly where the problem lies: the development of the information Government is much too *de facto*; it is too much the sum of decisions taken with respect to individual applications and policies without much thought being given to an overriding awareness of the larger whole. There is no language describing that awareness, and it certainly cannot be found in the discourse of eGovernment. Indeed, it is the eGovernment discourse that is depoliticising, instrumentalising and neutralising developments, even as the developments themselves require just the opposite.

8.2.2 iGovernment

In order to analyse the developments described in this report and provide guidelines for a new policy, we must begin to use the designation 'iGovernment'. In the words of Mayer-Schönberger and Lazer (2007: 5), the term iGovernment ('information Government') is a "conceptual lens that offers a complementary perspective to understand the changing nature of government and its relationship to the citizenry". It therefore refers not only to the *factual existence* of another kind of government owing to the developments we have described, but also represents another way of looking at that government. In iGovernment, the emphasis is on information flows and only in the second place on the technology that makes these information flows possible. This is an extremely important point, because political and public debate in the Netherlands always starts – and often ends – with

Figure 8.1 iGovernment depicted



the technology or even the specific technological application. By emphasising information flows, the conceptual lens of iGovernment also shows that the trends and developments covered in this book are more closely interrelated in everyday life than a discussion of individual techniques and applications suggests. Finally, viewing events through the conceptual lens of iGovernment reveals that, despite a few very modest attempts, the Dutch government is as yet unaware of the existence and implications of iGovernment, and is therefore unable to review and guide events within and outside government based on such awareness. That awareness is needed because there are two characteristics of the *de facto* evolution of iGovernment that, when combined, are undesirable, namely that iGovernment presents a paradox of political control and that it implies that there may not be any natural limits to the evolution of iGovernment.

8.3 THE PARADOX OF iGOVERNMENT

The political paradox of iGovernment is as follows: iGovernment has not been legitimised by explicit political decision-making, but is the result of many political and policy-related choices pertaining to individual technical applications and connections between applications and/or systems. At the same time, however, these individual choices are not simply a series of coincidences; they are in fact deliberate political and policy-related decisions.

8.3.1 POLITICAL CHOICES RELATING TO APPLICATIONS CREATE iGOVERNMENT

iGovernment has its origins in the actors who recognise and seize the new opportunities that ICT offers to meet their responsibilities and achieve their aims, and who develop and use the relevant tools. In many cases, they offer up a whole list of reasons for using ICT to achieve a particular policy objective, with the driving principles of security and effectiveness/efficiency being foremost among them. 'Techno-trust' and the desire to 'sell' systems politically also play a role in their arguments. Our analysis shows that this results in a wide variety of initiatives, each of which is in fact managed and assessed in political and policy-making terms. Each and every case, however, relates to isolated decisions relating to separate applications, ICT programmes and policy objectives. Only rarely is any thought given to the information flows generated via these applications and how these flows and their contents take shape in the larger complex of government information processes. In many instances, the decision-making process is repeated at a later date for yet another connection or to give yet another organisation access to information flows, once again on an individual-case basis. Function creep is a protracted but to some extent predictable process. The general public and government itself often appear to be entirely unaware of the scale on which information is linked and the impact thereof. Although there is often concern about separate information flows within a single policy area, about the informa-

tion flow generated by a specific application, or about an individual connection, no one considers the significance of connecting information flows further down the line, when they pass through various policy domains and are absorbed into more extensive information networks.

8.3.2 NO POLITICAL AWARENESS OF OR DECISION IN FAVOUR OF iGOVERNMENT

Not only are senior policymakers and politicians insufficiently concerned about or aware of the changes taking place, but there is also, for that reason, no framework for properly guiding such changes. It is more accurate to say that iGovernment has 'evolved' than to claim that it has been 'engineered'. It is precisely the absence of an underlying design that has allowed a complex and differentiated system of formal and informal policy, development and implementation processes to arise that differ from one measure and policy issue to the next. An entire fabric of information flows has emerged in each ministry and for each measure and system, without any natural limits being indicated. In fact, no one has even begun to consider what the evolution of iGovernment means for how government functions, how processes should be set up, and how government and the citizen relate to and view each other. The reality of iGovernment is far outstripping the political and administrative framework within it which it should be operating.

8.4 iGOVERNMENT WITHOUT LIMITS

The accumulation of ad hoc decisions and the absence of 'awareness' are permitting iGovernment to evolve without boundaries or limits. No one has restricted the dispersal of individual applications or the linking up of information flows, because no one has claimed stewardship of the whole. The tendency to specialise and divide issues into well-established political and administrative categories, as well as the associated financial and other interests, prevents a broader orientation. The question then is: who is responsible for evaluating and – when necessary – setting limits to iGovernment? For each of the observations below, we must therefore ask ourselves: how far should developments be permitted to go?

Our first observation is that it is mainly driving principles such as effectiveness/efficiency and security that are propelling the introduction of technological applications and the connections between them. Certainly in the wake of 9/11, government has set up many databases for security and control purposes in an effort to prevent a repeat of the disaster. The dynamic relationship between Justice and Home Affairs within EU policymaking is a good example of how the protection of personal data has, time and again, been forced to give way to security concerns, with Parliament exercising only a minimum level of supervision. But 'techno-trust' has also prevailed in recent years, pushing such popular phenomena as predictive policing and proactive management of citizens' future behaviour to the

foreground. That has, in turn, put pressure on such concepts as 'innocent until proven guilty' and 'forgiving means forgetting' in the criminal law. The emphasis on effectiveness/efficiency and security means that the underpinning principles of freedom of choice and privacy have generally been side-lined. When it comes to individual applications and connections between databases and systems, one can always find a good reason (usually political) for letting security outweigh other considerations – necessity knows no law, after all. But if no one is aware of the result at an aggregate level, the sum total of all those individual reasons will never be taken into account. That is why the absence of limits is most obvious when we shift our perspective from individual applications to iGovernment as a coherent entity. Although the politicians and policymakers involved do weigh up the principles underlying each new application or initiative, for example security, privacy or freedom of choice, that process does not involve their assessing these principles at the level of aggregated information flows, i.e. at the level of iGovernment as a whole – even though the application will ultimately become part of the evolving iGovernment.

The absence of limits can also be seen in the growing overlap between the policy domains of service, care and control, with the pace of digitization in the latter two domains having been particularly rapid. The emphasis on effectiveness/efficiency and security makes it appealing to break down barriers between different information flows in order to increase security, expand the scope of control, or streamline services. It also makes it easier to defend such measures politically. As Part II illustrated, the domains of care and control (social safety nets) are being 'mixed' in the youth care sector; control and service are crossing paths in various Internet initiatives launched by the police; and the development of the eLicence is keying into new ambitions related to both service and control. Facilitated by unique ID codes (including the BSN and biometrics), it has become possible to link a whole array of facts to a person and to share that data beyond the boundaries of what used to be isolated policy contexts and a restricted institutional setting. That data can then be combined with other facts and used in a new context. Influenced by these trends and developments, organisations are reassessing their own role and aims. Occasionally that means that they adjust their work processes and extend their scope of activity by developing new products and services in areas of policy where they had previously not been active. Viewed from the perspective of information flows and data use, the three policy domains of care, control and service are increasingly becoming an integrated component of public administration, even though they are in no way comparable or easy to integrate in terms of their administrative infrastructure, accountability mechanisms, legal rules and other frameworks. As a result, tension arises regarding duties, powers and responsibilities, in particular because former 'outsiders' (including private-sector parties) suddenly become involved.

8.5 THE IMPLICATIONS OF iGOVERNMENT WITHOUT LIMITS

iGovernment 'without limits' poses certain risks and problems, not only directly, but also because opportunities to harness the potential of iGovernment are ignored or not fully exploited. As iGovernment continues to evolve, a number of these risks must be addressed.

8.5.1 DISTORTED IMAGE

The first risk is that the solid basis government believes information technology will give it in a particular policy domain may turn out to be quite the opposite within the overall context of technically linked information systems. In the system-by-system approach described above, new applications are assessed individually and in isolated policy contexts, rather than in relation to the existing technologies and applications and the information networks in which they will be functioning. As a result, there is no clear picture of or critical reflection on the wider implications of any specific initiative. Ultimately, the image that government has becomes distorted in this way. It fails to sufficiently identify, acknowledge and review the underlying and broader interests or the problems and risks that are bound to arise when separate initiatives are combined. Being blind to the implications of combining information flows may lead to unpleasant surprises. Identity fraud is one example. It is a relatively minor phenomenon at the moment, but we have only just begun to take stock of the underlying problems. Combining, processing and decontextualising information are all processes that affect the quality and reliability of that information. Although the aim is to increase control, poor information quality can cloud government's view, cause its institutions and agencies to mistrust one another, leading instead to deterioration in control. There is a growing list of unfortunate cases: mistaken identity, incorrect and obsolete records that have material consequences, citizens who get bogged down in digital government networks. The risk is that politicians and policymakers will lose the ability to orchestrate matters; they will then have to do what they can to prevent the negative impact of an ad hoc iGovernment from outweighing the benefits of ICT.

8.5.2 NECESSARY ORGANISATIONAL AND INSTITUTIONAL CONTEXT IS LACKING

The second risk is related to our observation that the current discourse concentrates on technological systems instead of organisational processes. The focus, in other words, is on the product, and not on the process. The political and administrative debate is geared to an application, and sometimes even to a single aspect of an application, for example the security of the public transport chip card. As a result, the discussion ignores the wider process and the information network to which the application will be added – both immediately upon its introduction and later on, when decisions are taken to create links to other systems. The debate therefore

often focuses on the technical possibilities, whereas the organisational and institutional contexts are never considered or fade into the background. And yet it is precisely this context that is of vital importance for ensuring that the system, once it is operational, actually meets the public's quality standards – specifically the process-based principles of accountability and transparency. It will be highly problematic if iGovernment becomes so dominant that organisations are linked in terms of information flows but not in terms of institutional arrangements. Questions relating to accountability and transparency must be taken up on the scale of the overarching iGovernment, both legally and organisationally, in order to prevent these principles from falling through the cracks of the current organisational structure. Supervision and control are largely tailored to eGovernment and are organised, as a matter of either policy or law, to the partitions of the individual policy areas. The broader view of iGovernment is at odds with the way in which ministries, Parliamentary committees, regulatory bodies, and legal protection and complaints procedures are set up. It is vital, however, for citizens to know who is accountable; it is vital for government to know this too so that it can safeguard the quality of information and ensure the trust of citizens in iGovernment in the longer term.

8.5.3 TRUST AND INNOVATION

The third risk is that a lack of boundaries will eventually undermine the citizen's confidence in government as a reliable custodian and user of information. If there is no serious consideration of the features and requirements, and also of the new risks, of iGovernment, then government becomes vulnerable in its belief that technology works perfectly, but also because digital systems have become a vital infrastructure (risk of system and information failure). Without such reflection, matters such as transparency, accountability and good commissioning practices are at risk, whereas it is precisely these qualities that promote trust in government. Government must be able to ensure that information flows within its own systems – and to a certain extent outside those systems – do not become so unmanageable that they end up harming citizens.

Although it is too soon to draw clear-cut conclusions, the public's trust in government is already showing some cracks. There are various examples: the numerous objections to the EPD; the aggressive campaign of the grassroots movement *Het Nieuwe Rijk* ('The New State'), which distributed a parody of a government leaflet calling on citizens to have the BSN tattooed on their arms; and the court cases initiated by organisations such as *Vrijbit* ('Freebit') and Privacy First against the national fingerprint database of all Dutch passport holders. Still, the public in the Netherlands appears relatively untroubled compared with neighbouring countries such as Germany, where grassroots movements are very active in this area. Headline cases such as the T-Mobile affair in Germany and the major breaches of data security in the UK can severely test the public's confidence in government.[6] That

confidence could also prove to be fragile in the Netherlands. The survey commissioned by ECP-EPN and the WRR has in any event shown that public opinion on the use of personal data is closely related to the specific context of and reason for that use (Attema & De Nood 2010: 2). These results too show that government must acknowledge the importance of limitations.

Trust-related risks are not only a factor in the relationship between government and the citizen, but also within government itself, in particular in the relationship between policymaking and policy implementation. Both the ministries (policymakers) and the agencies and other government bodies at the operational level (policy implementation) have expressed a strong need for clear guideposts, in part in order to make practical management possible. It is precisely the lack of iGovernment self-awareness among policymakers and politicians and the absence of frameworks for its ongoing development that appear to be increasing the gap between policymaking and policy implementation. It is crucial to address that gap, not only in order to guarantee government's (and therefore iGovernment's) ability to act decisively, but also to retain the trust of the various parties within government itself.

Government also needs to be trusted if it is to pursue innovation. After all, to take advantage of all the opportunities created by well-considered iGovernment requires the ability to use technology and information to innovate. Innovation is always accompanied by uncertainty, and coping with that uncertainty requires trust.

"By definition, innovation is unpredictable and innovation policy must take that into account. This inherent uncertainty means that it is impossible for effective innovation policy to identify objectives and means in advance. It also means accepting that there will be frequent failures, which are a necessary part of arriving at valuable innovations" (WRR 2008a: 9-10).

Trust is needed to be able to accept the uncertainty that accompanies innovation and the failures inherent in the innovation process. The public must feel confident that the responsibility for potential failure is fairly allocated, and that no unnecessary risks are being taken. The uncertainty and failures inherent to innovation are only acceptable if innovative processes take place within a clearly defined framework.

8.6 Self-aware iGovernment

During the course of our analysis, we have reached the following main conclusion: the use of ICT and, in particular, of information/information flows is bringing about major changes in both policymaking/policy implementation and social real-

ity, which means that, in effect, a different government is now evolving. That new government is what this book calls 'iGovernment'. It is the nature of the new iGovernment to focus on information flows and related processes. Technology is not the leading factor here; rather, it is a facilitator. Our analysis shows that iGovernment is being created through the incremental accumulation of *de facto* initiatives that are insufficiently acknowledged or questioned by the relevant actors. Although iGovernment is still developing and growing rapidly, and although it has scarcely made any impression on politicians and policymakers, it is already having a very real impact, as our empirical analysis shows. At the same time, the lack of 'awareness' means that the features of iGovernment are scarcely taken into account in policymaking, and that politicians and policymakers do not sufficiently realise precisely *what* is developing, let alone *how* they can guide the development process in the right direction. What they require is a different perspective. All the evidence indicates that iGovernment will continue 'naturally' in the same way that is has evolved so far: it will develop organically through the continuous amassing of applications and information flows.

A shift in focus is needed to correct the failing awareness of this process and its consequences. Specifically, the focus must shift from the product – i.e. the application – to the process that it brings forth: the information flows. The many different information flows and their implications for policy and for society must be taken into account, not only in policy itself but also in the procedures and guarantees that have yet to be discussed. At the most basic level, that means the following:

Government as a whole must realise that ICT is transforming it from eGovernment into iGovernment. iGovernment makes different demands than eGovernment on how policy is used, how government institutions function, and what guarantees are extended to citizens.

As argued earlier, viewing things from the perspective of iGovernment reveals a number of problems in the way eGovernment currently operates. Specifically, we have only a vague, inadequate notion of the entire web of interdependencies, and no proper political or institutional framework for them. The following chapter therefore describes how 'iGovernment self-awareness' can help government consider how to deal more consciously and even-handedly with these problems. It not only suggests normative and procedural methods to encourage self-awareness, but also gives pointers for embedding iGovernment institutionally.

NOTES

1 Interoperability means that systems (or applications) are capable of exchanging data and/or communicating with one another. Interoperability requires standards, protocols and procedures.

2 Privacy Enhancing Technologies (PETS) is the collective name for various technologies built into information systems to support the protection of personal data.

3 Privacy by Design is based on the principle that designers, at an early stage in the design process, must consider the proper use of personal data within an organisation, the necessity of using that data, and how to protect it. Data protection, including PETs, should be incorporated into the design of the information system's architecture from the very start.

4 A victim of identity fraud, Ron Kowsoleea was wrongly registered in government information systems as a hard-drugs criminal for thirteen years. It turned out that a drug addict had stolen his identity. Kowsoleea was consequently identified as an irregular alien; he acquired a criminal record and fines for no reason; he had trouble travelling through Schiphol Airport; and the FIOD (Tax Authority Investigation Agency) raided his home while his two children were present. An enquiry by the Office of the National Ombudsman showed how difficult it was for the police, the courts and the border police to remove the incorrect records (National Ombudsman, press release of 23 October 2008).

5 Data mining is also referred to as the "predictive analytics of knowledge discovery from databases". Without data mining, data analysis is restricted to a small number of aspects that are thought to play a role. The use of data mining expands the scope of data analysis enormously. Artificial intelligence, statistical analysis and visual reporting methods can reveal all the hidden patterns and relationships, making it possible to analyse large datasets and discover complex connections.

6 In Germany, more than 17 million customer datasets were stolen from T-Mobile in 2006. The data included mobile telephone numbers (including unlisted ones), addresses, birthdates and e-mail addresses. All this data was offered to criminals via the Internet. There were a series of breaches of data security in the UK in recent years (i.e. secure information that was unintentionally made available in an insecure context). The cases included the loss of two computer discs storing data on 25 million child benefit recipients (November 2007); a stolen laptop with personal data on 600,000 Royal Navy recruits (January 2008); six stolen laptops with data on 20,000 patients (June 2008) (www.bbc.co.uk, consulted on 22 January 2009).

9 RECOMMENDATIONS: WORKING ON iGOVERNMENT

Government must become aware that it has developed from an eGovernment into an iGovernment. That awareness is essential if it hopes to meet the challenges of unremitting digitization and to use digitization to exploit the benefits of innovation. A rationale based on iGovernment self-awareness will require government to look beyond technology and individual applications and shift its view to a broader perspective on information. That broader perspective means focusing on the information flows that result from the many different applications and the connections between them. In particular, it also means considering the consequences for society and policymaking of the ongoing expansion and specific dynamic of iGovernment.

It is tempting to assign the task of accomplishing the necessary transformation and related measures to a particular ministry, organisation or official, i.e. to assign responsibility to a single entity or person with an overall view of iGovernment. That is largely impractical, however, given the scale, complexity and multifarious implications of ICT for the relationship between government and the citizen. This book cannot provide a comprehensive strategy or blueprint for arriving at an evenly balanced development of iGovernment, nor do the authors expect 'government', understood as a single entity, to do so. iGovernment self-awareness and the consequences of that awareness will have to sink down through the many levels and institutions that make up government, i.e. the ministries, agencies, local authorities, police, regulatory bodies, citizens, and – last but not least – politicians. iGovernment has evolved in many different places within government, and awareness of its consequences will have to do so as well. Be that as it may, it is naturally also true that, as George Orwell put it, "all animals are equal, but some animals are more equal than others." The current chapter will suggest a number of organisations to take on the responsibility of promoting this awareness and guiding the evolution of iGovernment in the right direction. These 'duties' should be viewed as the organisational side of an agenda of government transformation. The transition from eGovernment to iGovernment requires a paradigm shift that can be detected in the real-life developments described in previous chapters, but that must now, crucially, be embedded in the institutions of government and their thinking. That transformative *agenda* is much more important than any specific suggestions relating to the institutions themselves. Many roads lead to Rome, but government cannot afford never to arrive in Rome at all.

The first three sections of this chapter make a number of normative and procedural recommendations. Section 9.1 begins by offering recommendations for the tripartite division into driving, underpinning and process-based principles presented

earlier in this book, which have played such an important role in our empirical analysis. Based on that analysis, Section 9.2 describes three properties of information that should serve as warning flags for self-aware iGovernment. These are not *categories* of information, but *features* of information processes that require special guarantees both for government itself and for its relationship with the citizen. Such guarantees form the basis for the two recommendations made in Section 9.2; these, in turn, provide a basis for reflecting on the limits of iGovernment, as recommended in Section 9.3. Finally, Section 9.4 and Section 9.5 describe the components of an institutional framework for embedding 'iGovernment self-awareness'.

9.1 WEIGHING UP THE DRIVING, UNDERPINNING AND PROCESS-BASED PRINCIPLES

As experience has shown, the dynamic relationship between the driving principles (notably, effectiveness/efficiency and security) and the underpinning principles (notably, privacy and freedom of choice) is a defining factor in the evolution of iGovernment. In addition, process-based notions such as transparency and accountability point out the difficulties of creating a normative and institutional context for the development of iGovernment, as well as the opportunities that such a context creates. When put on the spot, every official – whether policymaker, politician or public servant – will attest to the importance of *all* these principles. After all, they appeal to common sense, responsibility, fundamental values, and due care. No one opposes security or privacy, for example, the two concepts that are most often played off against one another. And no one will deny that these principles should be weighed up carefully against one another. The decision-making process must, after all, be evenly balanced; decision-makers must look at all sides of an issue. When it comes to the theoretical foundations, then, there is general consensus. The everyday reality of government is often very different, however, as Part II of this book has made clear. As noted in previous chapters, ICT should be seen as a political choice and, as such, as more than a purely instrumental solution to a problem. When all is said and done, politics is strife. In the real world in which iGovernment is evolving, the process whereby politicians and policymakers weigh up the various principles is a less evenly balanced and public affair, as a rule, than theory might lead us to believe. There are a number of reasons why that is so: first of all, the principles are seldom discussed explicitly and openly; secondly, the principles are dissimilar and therefore difficult to pin down and weigh up against one another; and finally, a skewed presentation of issues can be advantageous in politics and policymaking. We look in detail at these reasons below and propose two recommendations for making the rationale and the debate on iGovernment more open, explicit and realistic with respect to the associated principles.

The three clusters of principles described in this volume – driving, underpinning and process-based – should be well balanced at all decision-making levels. That is no mean task, given that a quasi-quantitative concept such as efficiency, a more normative concept such as freedom of choice, and a process-based concept such as accountability all clearly fall under different registers of analysis. Furthermore, driving principles such as efficiency and security need very little encouragement to claim the limelight, as experience has shown.

That is often otherwise when it comes to the underpinning principles. These are grounded in civil liberties and individual autonomy and are enshrined in the principles of privacy and freedom of choice. Although the concept of freedom seems fundamental and absolute, such notions are in fact much more pliable in everyday life than the arguments that weigh in on the other side of the scale, i.e. efficiency and security. The argument that we must embed such principles institutionally is often prompted by the fear that individual interests will be harmed; that fear tends to lose out when weighed up against the perceived interests of the collective. In other words, the privacy of an individual is often not as important as the safety and security of the collective. Regulatory and judicial reviews virtually always focus on whether the infringement of a fundamental right is proportional. Valuable as the notion of proportionality may be, it runs into the difficult that there is really no common unit of measure or currency that allows us to make a quasi-mathematical comparison between dissimilar clusters of principles (driving versus underpinning). The problem with squeezing such a comparison into one particular straightjacket – for example a cost-benefit analysis – is that the arguments (and the language) of effectiveness/efficiency tend to prevail.

In everyday life , finding the right balance between the driving and underpinning principles of iGovernment often depends on the degree to which the intermediary, process-based principles of accountability and transparency have been put into effect. Without a sound application of these principles, no assessment is guaranteed a solid foundation. The principles of accountability and transparency must ensure the validity of the process by which iGovernment develops. Together, these principles require the implicit choices made by government to be made explicit: clear, comprehensible, open to discussion, and susceptible to objection. In fact, the only credible way to weigh up the various principles against one another in this context is by means of argumentation. In order to give such argumentation free rein, government must explain its rationale publicly at every level. One of the most important agenda items for iGovernment is that government must be required to explain, explicitly, how it weighs up the principles involved (a process that is unavoidable). That process must be laid bare at all levels, from the preparation and introduction of a specific application to the comprehensive diversification of processes and information flows that form the building blocks of iGovernment. Government must explain its rationale not only at the national

level, but also with respect to the decisions it takes at the international and, specifically, at the European level. That requires the Dutch Government to clarify well in advance what rationale it intends to bring to the European conference table and what results, in terms of that rationale, it hopes to take back home. This brings us to our first recommendation.

An evenly balanced development of iGovernment requires the driving, underpinning and process-based principles to be properly weighed up against one another in a manner that is clear, verifiable and can be publicly accounted for.

There is an urgent need for government to weigh up the various principles comprehensively and publicly, as doing so will help it avoid the undesirable consequences that may ensue from a unilateral approach to iGovernment. Ultimately, the single-minded pursuit of one principle only (whether it be security, privacy, transparency, or any other) means that iGovernment will gradually – application by application and link by link – take on an extreme, impractical and vulnerable form. It is therefore important to keep an eye out for signs and warnings that one or more of these principles are set to stifle the rest. After all, society can have too little of a specific principle – but too much as well. The potential danger of domination applies to *all* principles, especially when taken to extremes: driving principles such as effectiveness/efficiency become economic reductionism; underpinning principles such as freedom of choice become choice overload; and even a process-based principle such as accountability can result in excessive mistrust and litigiousness when applied unilaterally. But even the 'midfield' – between the two extremes – requires a proper balance. Too much emphasis on security may soon be at the expense of privacy and transparency. Too much emphasis on privacy, on the other hand, may be at the expense of transparency and accountability, as accountability always requires a certain degree of openness. All too often, initiatives have gone ahead without a genuine, meticulous and verifiable comparison between these dissimilar principles. The comparisons that have been made – for example as explained in parliamentary documents – are often fragmented and/or superficial.

That is not only due to the conceptual difficulty of reaching a credible balance, of course. The principles must be weighed up at different moments, at a variety of different levels, and in the many different processes and procedures that together result in iGovernment: in a parliamentary debate about a new application; when describing the work contracted out to an applications designer; when deciding to link files or connect new organisations to a network; and in the rulings and opinions of the courts, regulatory bodies, and citizens regarding new developments and decisions. There is much at stake in each of these situations, and one can at times witness a tendency to allow a single principle to overrule the others simply in order to be done with a dispute or avoid a dispute in advance. It has happened numerous times in the course of iGovernment's evolution that plans for a new

application were unveiled in a way closely resembling a marketing campaign. At times, 'techno-trust' is not really trust *per se*; it is really more of a political sales pitch. A little less hocus-pocus with terms such as effectiveness/efficiency and security would be advisable. But realistic and verifiable arguments and comparisons are also lacking at the other end of the spectrum, for the underpinning principles of privacy and freedom of choice. If something has to be sacrificed at that end (and that is often enough the case), then the 'loss' should be acknowledged and communicated as such. In other words, although in most cases it is not clear in advance what the 'right' balance is between the driving and underpinning principles, the debate on this question is in sore need of improvement.

Discussions as to how iGovernment is to evolve further and the role that the principles should play in its development must be more solidly grounded in reality. So far, neither those who emphasise the opportunities nor those who emphasise the dangers have argued their case entirely credibly. The process-based principles of transparency and accountability can play an important role in this respect. A sound and credible process-based framework for iGovernment can help ground the discussions about the direction that should be taken in reality. The arguments relating to the underpinning principles must also be made explicit and as verifiable as possible. It particular, it would be more realistic at this end of the spectrum to cease regarding privacy and freedom of choice as all-or-nothing principles. Sometimes it is in fact necessary to sacrifice a degree of privacy or freedom of choice, provided that the sacrifice is made clear and there is good reason for it. Government should not, after all, pass up every opportunity to use modern technology and scientifically sound methods of risk assessment, diagnosis and intervention to protect human lives (Buruma 2011). Too much privacy may mean that the authorities never become aware of a child at risk; too much freedom of choice in a complex situation may leave citizens empty-handed after all.

Clarifying the driving principles and making them as verifiable as possible would in turn raise two issues and open them up for discussion. The first of these is the often unjustified optimism among politicians and policymakers about what ICT can do, as the cases cited in previous chapters and in many other studies have shown. Although optimism often drives innovation, in the Netherlands it has led to ad hoc projects, impossible deadlines, and expensive ICT failures. The second issue is that 'spill over' and 'function creep' are often quietly calculated into the equation from the very start of project. Officially, politicians distance themselves from such 'fiddling' and reject it in their discussions and debates, but they are in fact fully aware that the future is likely to bring precisely the thing that the Government is officially ruling out at an earlier point in time. The formal argument then is that political responsibility only extends to the proposal at hand, and not to the possibilities that the proposal holds out (implicitly, but without requiring too much imagination). When iGovernment consists of a chain of such

isolated decisions, reasoning of the 'after us, the Deluge' kind is simply untenable. Real iGovernment self-awareness requires politicians to take the expression 'a government forewarned is a government forearmed' seriously in the digital domain, and to apply this philosophy to implicit but foreseeable ICT trends. Government often anticipates the future in its policy, and it would be to its credit to do the same, and to do so openly, in its political assessments of iGovernment.

9.2 WARNING FLAGS FOR iGOVERNMENT

As the process of digitization continues, it is important for government to be much more aware of certain features of information than is now the case. The point is not to focus on the information *content*, as is so often the case (with DNA data requiring a higher level of protection than biometric data, for example, and biometric data requiring a higher level of protection than simple personal data such as names and addresses). Although it is important to break down information into content-related categories – as indeed happens in many of our existing laws and rules – this book focuses on information *processes*, precisely because they have a huge impact on the nature and the reliability of the information that keeps iGovernment running and on which it depends. In today's digital era, these processes have a number of features that must be taken into account when considering how to expand or set limits to iGovernment in a way that is evenly balanced.

We have therefore tagged three interrelated processes with warning flags. These warning flags are not intended to be prohibitions; rather, they are a sign that policymakers and politicians must be extra vigilant. They will help improve general 'iGovernment self-awareness': when information is either part of or the result of the tagged processes, government must pay close attention to the quality of that information and consider who bears responsibility for it. In some cases, the conclusion may even need to be that it is necessary to impose certain limits on the use of information. An evenly balanced development of iGovernment requires us to look very closely at these information processes. The three processes that we have flagged in this way are:

a The *networking* of information, i.e. the shared use and management of information within a network of actors.
b The *compiling and enhancing* of information, i.e. creating new information and profiles based on different sources from different contexts.
c The pursuit of a *preventive* and pro-active policy based on information, i.e. actively evaluating and intervening in society founded on an information-driven risk calculation.

These three information processes are the core of iGovernment, enabling it to fine-tune and customise policy, obtain a comprehensive picture of the public and of the policy issues involved, and take pro-active action where needed. At the

same time, they are processes that themselves have an impact on information: they influence its nature, reliability, recognisability, contextuality and traceability. Although there are no insurmountable or absolute objections to this, it is important to make sufficient allowance for the risks involved in these processes when dealing with and using that information or when allocating responsibility for it. That is very often not the case given that iGovernment lacks self-awareness. It is important to realise – much more so than at present – that it is precisely these three processes that have a big impact on (a) the quality of information *content* and (b) the demands made on the *organisational context* of information flows. Consequently, there are a number of important conditions that can be identified for the ongoing development of iGovernment.

9.2.1 QUALITY OF INFORMATION CONTENT

All three information processes – the networking of information, the compiling and enhancing of information, and the pursuit of information-driven preventive and pro-active policy – require a critical assessment of both the quality and the relevance of the information produced by the systems of the various authorities. Part II discussed various tendencies and reflexes, for example: the nonchalant linking up of information files; the habitual overstepping of the boundaries between the service, care and control domains; the absence of a clear and pre-determined plan to control the unstoppable flood of information; the continuous dilution of information quality owing to repeated use; and the accumulating and mixing of many different kinds of information. In iGovernment as it has evolved in recent years, composite information circulating in networks easily crosses 'boundaries'. Those boundaries are not only territorial ones (the borders between countries), but also, and in particular, the dividing line between public and private sectors and 'their' information, and the distinction between information used for service, for care, and for control purposes. Much of this information is, moreover, decontextualised when it is retrieved from its original environment, only to be recontextualised when combined with other data in a different policy context. That naturally has consequences for the reliability and recognisability of the information. These consequences are not only felt by the professionals who work with the data (and who are obliged to interpret information taken from a different professional context), but also apply, to an even greater extent, when the information concerned is the result of technological 'reproductive processes', such as profiling and data mining. The more data and information files are contaminated – and they often are contaminated, or at least vulnerable to being so – the more networks will increase exponentially any risk associated with contaminated information due to the unique dissemination characteristics of networks. A contaminated information system will not grind to a halt on its own, after all. On the contrary, in many cases no one is even aware of the diminishing quality of the information, and it continues to be processed and reprocessed, used and re-used, again and again.

Meanwhile, both the relevant government official and the citizens in question are unaware of the deterioration. It is all too easy for the quality gap to remain unnoticed, especially in networked situations, without anyone being 'to blame'. Indeed, this may well be an unavoidable risk of what can be referred to as the 'multiplier effect' of ICT: information circulates and is effectively distributed at lightning speed, whether or not it is correct. Administrative reality and 'real reality' can diverge quite dramatically in iGovernment, and errors can be disseminated much more quickly, making them more difficult to rectify later on. Such errors can have huge repercussions for the daily lives of individual citizens, especially if profiling is used to enhance information or pursue a pro-active policy based on faulty data.

The quality of iGovernment therefore requires constant attention and consistent policy across the breadth of government. The assumption that information is correct must be replaced, across the board, by the realisation that some information is very likely to be inaccurate, obsolete, or even misused and manipulated. The default position within government, however, is that the system always tells the truth; margins of error are ignored and citizens are increasingly held responsible for the problems that ensue. There is too little awareness of the consequences of iGovernment; the multiplier effect and the constant decontextualisation owing to the networks are not factored into the monitoring of information quality, if such monitoring takes place at all. Policymakers can also be blinded by the positive results of networks and composite information. Their concern about the quality of information should not be limited to the information itself, but should also extend to the metadata. Metadata acts as an indispensable signpost in information management systems. It plays a crucial role in tracing information and identifying the original context and origins of that information. The quality of an iGovernment information management system depends on the presence of good quality metadata. In addition, the quality of the information depends on such technical and organisational prerequisites as data security, well-designed work processes, and a reliable authentication and identification infrastructure.

Government must do more than it currently does to counteract 'techno-trust', as evidence shows that every system and every information flow has both intentional and unintentional effects, and that those effects, in turn, influence the content of the information as such. All too often, government insists – and often does so officially – that its data is correct. In other words, government trusts too much in the quality of information and lacks a healthy dose of scepticism in that regard, adding to the vulnerability of iGovernment.

Self-aware iGovernment always looks critically at its own information management systems. It regards the quality of the information and of the information processes with a healthy dose of scepticism; both must be judged continuously on their merits and improved where necessary.

The role that information plays in policy processes changes once digitization is introduced. Increasingly, information is being used to anticipate the future, a trend that is also catching on in the areas of service, care and control. In a growing number of cases, the traditional method – whereby statistics are used to inform and improve policy – is being supplemented by information-driven policy designed to predict *individual* behaviour. Information and risk calculations are used to predict which children may be at risk and which passengers may be terrorists, for example. Action is then taken based on that risk calculation. The shift in focus to individual behaviour means that the outcome of a risk calculation may be very valuable – a life is saved or an attack thwarted – but it also means that the repercussions are extremely serious if the calculation is wrong. Anyone who is flagged in government networks and systems as a potential terrorist, criminal or abusive parent will feel the consequences in his or her daily life. There is too little awareness in government of the use of statistics and risk calculations in connection with individuals (rather than in connection with broad policy categories), and of the potential consequences of doing so.

The most dramatic examples with the most far-reaching implications are found in the area of national security and in care sectors involving life-threatening situations. But even in less precarious areas of service and care, statistical methods and the effects of networked information processing can assign individual citizens to the wrong category and retain them there for a lengthy period. These separate domains are also increasingly coming to overlap thanks to ICT, with errors being circulated and dispersed between them. It is clear as well that information is no longer as easily 'forgotten' in the everyday reality of government information management, despite the prescribed retention periods. Certain categories of personal information tend to persist in profiles and networks, with all that this implies for the individuals involved.

iGovernment must therefore keep a keen eye on the possible negative and even damaging effects of information-driven policy. Sound procedures for dealing with such policy are vital for those individuals who find themselves in a tight corner. They are also important as a way of maintaining and boosting confidence in iGovernment. They require an even balance between the principles of accountability and transparency and also require the roles and responsibilities of government and the citizen to be evenly balanced. It is important to distinguish between the role of the citizen as *citoyen* (a participant in the political life of the community) and the role of the citizen as an individual (someone who has certain legal rights and obligations). In the first instance, the citizen is a productive countervailing power who should be 'kept in the loop' as regards government policy and the role that information processes play within it. In the second instance, a citizen who is treated unfairly or improperly by government or who ends up trapped by the systems of iGovernment must be able to invoke his or her rights. Both roles require a certain

amount of vigilance – a combination of watchfulness and assertiveness – to act as a counterweight to the expansion of iGovernment. Citizens cannot be assumed, however, to exercise vigilance by default; they must be supported by rights and procedures that are, in effect, the practical outcome of taking the principles of accountability and transparency seriously. Generally speaking, the citizen-*citoyen* sees transparency as a greater priority, whereas the citizen-individual gives top priority to accountability.

In order to support citizens as a countervailing power, iGovernment must display a certain amount of openness about its affairs. Without transparency and access to information, real democratic supervision is impossible. That means that iGovernment must be more open and that it must encourage citizens to think and talk more about its development, and do so at earlier stages of its 'design'. Government must do so both of its own accord and in response to vigilant citizens and organised groups that have submitted requests and followed procedures in order to gain access to information. The platitude 'you have nothing to fear if you have nothing to hide' can just as well be applied – tongue in cheek of course (after all, it is just a platitude) – to iGovernment itself. As a supervisor of government, the citizen may justifiably be expected to be vigilant and assertive; equally justified, however, is the citizen's expectation that government should be more transparent.

When a matter concerns the citizen as an individual – and in particular when that citizen is seeking justice from the state – then transparency is only the beginning. Transparency will ease the way towards being better informed, of course, but an emphasis on transparency should not mean that the well-informed citizen is (erroneously) taken as the standard, thereby putting the onus on all citizens to get their digital affairs in order and to be unrelenting in their vigilance. The existence of a 'digital divide' alone implies that there would soon be enormous inequality between different groups of citizens. What is more, the citizen has neither the authority nor the power to change anything permanently in the networked back office of iGovernment. Experience shows that citizens are often the victims of back office errors and are powerless to correct them. It is important, therefore, to set up sound procedures relating to final responsibility for information and an unambiguous access point that enables citizens to induce iGovernment authorities to act accordingly. That involves striking the right balance between the citizen's responsibility to alert the authorities to inaccuracies (and his or her capacity to do so) and the authorities' responsibility to actually correct such inaccuracies. Particularly in the more sensitive domains of care and control (in which successes are extremely beneficial to society and errors are extremely disadvantageous to individuals), citizens should not be saddled with the unique responsibility for incorrect or obsolete government information (or its consequences). In short, government bears a heavy responsibility because it alone has the power to take binding decisions that will correct errors throughout

the iGovernment network, and not only in the particular database or organisation where the problem has been detected. On the other hand, the threshold should not be too low for individual citizens either, as it will then be too easy to require officials to go to unnecessarily excessive lengths.

iGovernment must invest in procedures that will improve transparency (supporting the citizen as citoyen) and accountability (supporting the citizen as an individual with legal rights and obligations). Right now, responsibility and accountability procedures within iGovernment are inadequate and insufficiently effective; responsibility and accountability must be identified and allocated more comprehensively, explicitly, and clearly.

9.2.2 EMBEDDING SUSTAINABLE AND FAIR INFORMATION FLOWS IN THE ORGANISATION

iGovernment self-awareness, and in particular the three warning flags of networked information, composite information, and information-driven proactive policy, naturally also have repercussions for the practical and organisational design of iGovernment. Despite the increasingly common use of the term 'information management', information flows are still not properly embedded in the organisation of government when it comes to management, quality, and the safeguards. The evolution of iGovernment has so far been 'a lot of flow, and too little management'. The flow of information throughout the organisation of government (and beyond) is growing freer, but the conditions for properly controlling and managing such flows are lagging behind. Converting paper files and filing cabinets into digitally linked information files offers new opportunities, but it also casts government's traditional duties and obligations in a different light. The work of organising and managing all the information circulating in government's databases and networks is qualitatively different to the work of managing information on paper. Information management also involves the way iGovernment's 'memory' functions, and that immediately leads to two problems. On the one hand, government is growing 'feeble-minded' and forgetting things that should not be forgotten. On the other, government increasingly 'remembers' information about citizens, the thinking being that such information may come in handy someday. The first is harmful because transparency and accountability are impossible without a good memory. The archiving function of government enables it to hand on, trace, disclose, and account for its actions. That is vitally important both internally, within government, and externally, vis-à-vis the citizen. In the digital era, however, archiving requires a radically different approach to government information management. The Netherlands Court of Audit has emphasised this repeatedly and offered various organisational guidelines to that effect.

At the same time, government appears to be incapable or unwilling to forget certain types of information. The inability to forget is also harmful, however, because it means that citizens may not be able to escape from their past. Government sometimes proves unable to observe its own prescribed retention periods; it is also inclined to extend these periods, based on the notion that more information equals better information. Security and fraud prevention are magic words in this respect, but there are also good reasons for government not to consider all of the past when judging citizens in the present or future. By working with profiles, government quenches its own thirst for information and makes the very act of storing and remembering information important in itself. People are much more likely to be seen as the products of their past than they were in the pre-digital era. If digital records are stored in perpetuity, 'once a thief, always a thief' takes on new meaning. The fact that it is technically possible to store personal data for ever is not a good enough reason to actually do so. Once again, we need to examine the pros and cons of storing (or deleting) information within the relevant context, and that examination may differ from one context to the next. For example, information that is used in criminal investigations may need to be scrutinised differently to information in the healthcare sector, where long-term data storage can be of enormous benefit for research and for estimating mortality risk and heredity. The next question, i.e. *how* the data should be stored (for example, whether or not it should be anonymised), is also one that should be considered and evaluated on a category-by-category basis. There is in fact not one standard for storing or forgetting all personal or other information (i.e. an *absolute right* to be forgotten); it comes down to government weighing up each situation properly and rationally and then acting in accordance with its findings. In short, it is vital to the ongoing development of iGovernment to take its 'memory' into account. The archiving function of government must be improved, and that will require a radical turn-around in thinking. In order to decide which citizen records should be 'forgotten', government will need to constantly set off collective interests, for example security, against individual[1] interests, such as the right to be forgiven and forgotten, and to do so transparently. To guarantee that it is acting fairly, moreover, government must be more aware than it currently is of the risks associated with using obsolete data. The Dutch Government must also ensure that the organisations operating within iGovernment are continuously aware of the importance of forgetting. Organisations must weigh up the two sides (remembering versus forgetting), make their arguments explicit, and see that the results of this process are given solid organisational foundations. iGovernment must also come up with structures and low-threshold methods for helping citizens remove obsolete, incorrect and inaccurate data.

iGovernment must have a memory that is effective, sustainable, and above all fair. The importance of storage and archiving demands a radical change in culture. The importance of forgetting must be permanently acknowledged and requires a strategy that is embedded both in policy and in the organisational structure.

9.2.3 IGOVERNMENT'S 'LIMITS TO GROWTH'?

When iGovernment is not self-aware, its natural tendency is to continue expanding. After all, only self-awareness can induce it to set limits to its own growth. Until then, there will be no real limits to the size of data collections or on the number of links between systems; information will become contaminated; organisations and information flows will be misaligned; citizens, businesses and even government organisations will become trapped in the tangle of government data; it will be difficult to prove one's identity; and it will be virtually impossible for citizens to extricate themselves from the information that is gathered, processed, and exchanged about them. Without iGovernment self-awareness and without an awareness of what iGovernment means for the relationship between government and the citizen, there is little reason or opportunity to consider the growth of the information structure that government is building. There is also little reason to ask questions, for example whether such growth is actually necessary, whether there is a need to set limits, and how iGovernment should continue to develop. Questions and concerns regarding the relationship between information flows and their implications will be left unaddressed even as the work of constructing iGovernment continues. But government is selling itself and the citizen short by proceeding in this manner. Moreover, both the citizen and government are left vulnerable.

The practical reality of information dissemination and linkage, and the reasonable expectation that claims will be made on data collections in the future, require government to engage in a broader assessment that (a) looks beyond any specific policy initiative that it may be considering and (b) looks beyond the current circumstances. The process of weighing up the various interests at stake in iGovernment also raises a more fundamental question: is the iGovernment that has evolved the iGovernment that we would have wanted if we had specifically planned and designed it in full awareness of the context and relationships involved? This raises another issue: are there limits to iGovernment? If so, where are those limits to be drawn, and where not? And how do we determine that?

The questions relating to limits also touch on a certain vulnerability of iGovernment that is best illustrated by the Internet. The fact that the Internet is, fundamentally, an unregulated and open network makes it virtually impossible to 'manage' it or to monitor the information circulating there. After all, anyone can access information once it has been placed on the Internet. Incorrect or undesirable information can be deleted from one's own site or perhaps (after legal proceedings) removed from someone else's, but by then it has usually already been copied and 'mirrored' elsewhere. The WikiLeaks case in late 2010 offers an excellent example of how information on a site is quickly copied elsewhere precisely because the authorities and other stakeholders wanted to restrict access to it.

The uncontrollable nature of the Internet and the fundamental consequences of such uncontrollability play a similar role with respect to iGovernment, in two different ways. First of all, they affect iGovernment itself, or more specifically, government's internal information management. That differs from the Internet in that it is a semi-restricted system and not an entirely open one. It is therefore possible to control information flows to a certain extent. However, the dynamic evolution of iGovernment today is putting pressure on that ever-so-slight controllability of information. Thanks to the networked nature of information and the merging of information flows across public-private boundaries, the semi-restricted system of iGovernment is growing increasingly similar *internally* to the Internet. A growing amount of information belongs to everyone in the system rather than to only a single organisation, making the job of properly guiding information flows virtually as difficult within iGovernment as within the Internet model.

As this trend continues, it will become more difficult for government to channel, verify and guarantee the reliability of information. Alongside the risk of iGovernment 'internalising' the logic of the Internet, there is another risk: that iGovernment will unintentionally become *part* of the Internet. The WikiLeaks affair once more provides a striking example, foreshadowing what will undoubtedly happen more often in future. Thanks to WikiLeaks, the authorities' internal information management system suddenly became public property on the Internet. Copied countless times and migrating rapidly from server to server and from cloud to cloud, information circulated beyond control. Dutch versions of WikiLeaks have already turned up that leak government documents anonymously and confidentially, for example *www.opennu.nl* (www.opennow.nl). Only methods such as those applied by the Chinese government might succeed in putting the genie back in the bottle, and even that is uncertain – to say nothing of whether it would be desirable. Before government information is actually leaked on the Internet, the risk of disclosure is thought to be a question of data security and the technology and policy required to effectuate it. Once sensitive information is leaked and disseminated on the Internet, however, policy is pushed aside and the authorities start to improvise in order to regain control. It is a rather unedifying sight. The pressure that the US government put on service providers to remove WikiLeaks from the Web led Amy Davidson of *The New Yorker* to ask whether "Lieberman feels that he, or any Senator, can call in the company running *The New Yorker's* printing presses when we are preparing a story that includes leaked classified material, and tell it to stop us. The circumstances are different, but not so different as to be really reassuring."[2] Nevertheless, digitization has made such leaks virtually unavoidable, and they will, unavoidably, become more frequent in the future: the 250,000 pages in the possession of WikiLeaks would have never been leaked in the same manner or on the same scale if they had existed only on paper. It is digital compression that makes information mobile and permits major leaks of

this kind. Many earlier notorious cases of leaked information, for example in the UK, also concerned huge volumes of personal data stored on a lost USB stick no bigger than a cigarette lighter. The fact that leaks are unavoidable – whether they are intentional or due to error, carelessness or gross negligence – and, in particular, the consequences of such leaks are reason enough to consider the limits to iGovernment.

Although we will not identify those limits in this book (that is a matter for politics), we can indicate the general areas that should be considered. Our purpose, in other words, is to raise awareness and to spark off a debate about such limits, and not to identify precisely where they are. After all, what was most valuable about the Club of Rome's report *Limits to Growth* was that it put the environmental problem on the political agenda, and not that it made precise predictions and extrapolations. The processes identified in previous chapters offer us some preliminary guideposts for identifying where the limits might lie: we are, in effect, being forced to think about the limits to iGovernment when we weigh up the various principles involved and observe the warning flags indicated. Although it has now grown common (albeit largely unnoticed) to mix service, care and control and to cross the boundaries between the public and private domains, these tendencies too turn out to be problematical when examined more closely and from the perspective of iGovernment. Finally, the realisation that the Internet has created a completely different information environment in which iGovernment too must function gives us every reason to analyse the nature of iGovernment and to act accordingly. Well-reasoned limits are extremely important here, not least because they give the authorities something to go on when identifying the right way to deal with information or to share it with other parties (even those in government). Right now, that is often left open to interpretation. For example, the Tax and Customs Administration decided not to exchange information within a partnership of various parties assembled by a local authority with a view to clearing a travellers' camp.[3] Tax and Customs did not feel it had the right to share sensitive information with an electricity company or other private parties; as a large, autonomous government department, it defined its own 'absolute' limits and pulled out of the negotiations. Another example is the Dutch Supreme Court's ruling (described in Chapter 7) on the Public Prosecutions Service's requisitioning of passenger data from Trans Link Systems.[4] It should not, however, be left to bottom-up campaigns or isolated judicial rulings to set such limits or to define the framework for the ongoing development of iGovernment. After all, if Tax and Customs or Trans Link Systems had agreed to provide the information as requested, the data exchange would have quietly taken place, without any further discussion.

A self-aware iGovernment cannot exist without there being a well-reasoned strategy regarding the limits to that same iGovernment. Such limits are required by both

the internal dynamic of iGovernment and the dynamic of the iSociety: without limits, government will ultimately lose the ability to guide the ongoing development of iGovernment in manageable channels.

9.2.4 AN AGENDA FOR THE TRANSITION TO A SELF-AWARE iGOVERNMENT

It is urgent that 'iGovernment self-awareness' become ingrained government-wide, both as a concept and as an organisational factor. The danger, however, is that such awareness will be cancelled out by the political issues of the day. Given what is at stake, that would be an unfortunate turn of events. In order to act on the recommendations given above, government must transform its existing system of public administration into one capable of identifying and tackling the challenges that iGovernment brings. The organisational and administrative effort involved will require the engagement of many different organisations and levels of government. In other words, our recommendations are not intended solely for the Dutch Government. The national authorities can, however, *drive* the search for solutions. In addition, iGovernment is now so dynamic that it must have sufficient leeway to rapidly integrate new developments and the responses to such developments into its thinking. 'iGovernment self-awareness' is not just a status to enjoy, but rather an ongoing challenge. In a world of rapid and dynamic digitization, however, it is important to create various champions that (a) claim stewardship of 'iGovernment self-awareness' and (b) provide iGovernment with a well-defined, authoritative point of contact and recognisable identity.

The institutional landscape as it now exists is not equipped to create such champions. At its core, iGovernment consists of interrelated information flows and networks – and it is precisely on that point that we lack organisations that are willing and able to concern themselves with the integrated whole. The political debate is broken down into laws, areas of policy, Parliamentary committees, and technologies; only rarely does it consider the overall information picture, let alone any existing or future links between information flows and their consequences. The same compartmentalisation applies with respect to the funding for digitization projects, and consequently for how funding is managed and influenced. There is no 'Ministry of Information' or 'Parliamentary Committee on Information'. Ministries, government agencies and other local and regional authorities are primarily concerned with their own policy problems and spare little thought for the consequences of incoming and outgoing information flows that reach beyond the 'limits' of their own duties and organisation. The same can be seen in cross-border contexts. The European network of information flows and personal data is expanding and diversifying without there being any frank discussion as to whether, how, and under what circumstances the Netherlands will participate in the emerging iEurope. Government agencies use the information they obtain in communication with citizens, but they are powerless to trace

errors in information flows and correct them throughout the entire chain or network when the same citizens run into problems. The many different supervisory bodies (for example the Data Protection Authority and the Office of the National Ombudsman) and other organisations such as the Identity Fraud Helpdesk, which identify and attempt to resolve some of the excrescences of iGovernment on behalf of citizens and government agencies, are often simply not equipped for the task in that their responsibilities do not reach far enough, and are in fact incapable of producing solutions (or at least lasting ones). Cross-ministry programmes and other arrangements, such as the Reinforcement of Public Sector Identity Chain policy programme (*Versterking Identiteitsketen Publieke Sector*, VIPS), are only temporary, and in many instances are not sufficiently high-profile in terms of bureaucratic stature. Not one of them has the authority to implement its methods or solutions permanently across the boundaries of ministries and institutions. Government also lacks the expertise needed at the policy-technology interface to develop new systems that are 'iGovernment-proof'. Brave attempts are made at all these levels to consider iGovernment in its entirety, to conduct proper assessments, and to search for solutions to problems, but the existing organisations and arrangements are unable to meet the challenges of iGovernment because they have not been assigned the necessary statutory duties or the authority to take binding decisions. There is therefore an urgent need to develop an agenda for institutional transformation. Government must catch up with practical reality by transforming itself institutionally from eGovernment into iGovernment. It needs institutions that will allow it to channel the discussion on the ongoing development of iGovernment in the right direction, to claim responsibility for its own networked information management system, and to provide citizens with a form of protection that takes the properties of iGovernment into account.

Fleshing out the targets for iGovernment will therefore require an institutional transformation that assigns and embeds three functions within government:

a the *strategic function*, i.e. guaranteeing the well-considered, ongoing development of iGovernment;
b the *societal function*, i.e. making iGovernment more transparent for the public and improving its accountability vis-à-vis individuals who become entangled in information networks;
c the *operational function*, i.e. improving well-reasoned connections between policy, implementation, technology, information flows, and networks. Also, improving the commissioning practices of government.

These three functions constitute the absolute minimum requirements for shaping iGovernment self-awareness and acting on the implications of the new reality. The following section offers specific proposals for these three functions, along with the necessary institutional 'mechanisms'. It should be noted that the institutional

transformation as such – which involves embedding aims and facilitating implementation – is ultimately more important than merely the labels for the organisations proposed here.

iGovernment requires the system of public administration to be transformed, with existing arrangements being redesigned at the strategic, societal and operational levels.

9.3 iGOVERNMENT INSTITUTIONS

iGovernment as it has evolved in recent years certainly does not lack for institutions. Our analysis in Part II of this book involved a procession of government organisations and did not even mention an equally large number of organisations that are concerned in various other ways with ICT and government. All these institutions and organisations do their work as best they can in their own specific area. The problem is that – like iGovernment itself, which has evolved largely without a pre-determined design or plan – many of them have also emerged spontaneously along with iGovernment or have been added piecemeal. In the same way that iGovernment has developed application by application and link by link, so too has the institutional landscape evolved in response to individual applications and the related opportunities and problems. These organisations are in fact eGovernment – and not iGovernment – institutions. However: they do not have the same relationships and links that are such important features of iGovernment. That is true both for the way they have developed and for the way they exercise supervision and enforcement. Although many organisations are dedicated to promoting the opportunities of ICT or to highlighting the disadvantages and risks involved, as a group they are not sufficiently effective. The individual organisations scarcely acknowledge that their own work is related to the work of the others, let alone explicitly refer to that relationship in their mission or in the action they take.

One important conclusion that we can draw from our arguments above is that the networked nature of iGovernment makes it extremely difficult to control from a central point. Hierarchies and networks are uneasy bedfellows. At the same time, something or someone must drive iGovernment self-awareness forward, the implication being that this should be a national body with the authority to take binding decisions. The challenge, therefore, is to identify institutions that can combine the logic of networks and the power to take decisions, within both government and the broader social context of iGovernment. iGovernment operates against the backdrop of an iSociety that is influenced by and in turn influences ICT. In addition, government's public information networks often flow over into the private networks of businesses and citizens. iGovernment cannot be structured autonomously and in isolation. All the relevant actors must be involved –

not only those within government but also stakeholders in the private sector and the citizen. The motto must therefore be: 'Make sure we involve the iSociety in building an iGovernment to last'.

If we follow this book's line of argument to its logical conclusion, then the only real institutional recommendation that we can make is that iGovernment self-awareness must seep down into every government organisation and into every vital point in the process of digitization, from the initial plans drawn up at the national or international level or the first sketches for a new application to the specific assignment or contract and, later on, to the linking up of information. iGovernment self-awareness must be ingrained throughout: that is the aim. Such awareness grows by means of an evolutionary process that can be accelerated by external factors, for example (as we have seen in other countries) the uproar surrounding the publication of confidential government documents by WikiLeaks, or a major scandal relating to information management. But the growth of that awareness can also be encouraged by establishing institutions specifically designed to act as drivers.

In this final section, we describe the general outlines of four institutions capable of driving iGovernment self-awareness. The strategic, societal and operational functions are allocated to four new organisations that must be given the power to shape the transformation of iGovernment. As indicated above, recognising the urgency involved and developing an associated agenda are more important than hammering out every detail. The biggest priority is to allocate the strategic, societal and operational functions to institutions and to equip these institutions with the necessary means and the power to take binding decisions. It is against this background that we make four proposals for iGovernment institutional innovation: to allocate the strategic function to a permanent committee for iGovernment that reports to the Senate and House of Representatives; to allocate the societal function to a national iPlatform and an iAuthority, the first being responsible for transparency and the second for dealing with and resolving problems that citizens encounter with iGovernment; and finally, to allocate the operational function to an organisation responsible for ensuring professional commissioning practices in government.

9.3.1 PERMANENT COMMITTEE FOR IGOVERNMENT

The responsibility for promoting iGovernment self-awareness must be allocated to a national organisation. That is because, in any scenario, there is too great a risk that such awareness will be dissipated among the particular interests of the various actors and organisations that concern themselves with ICT and its consequences.

Set up a permanent committee for iGovernment that reports annually to Parliament on 'the state of information'.

The main task of such a committee would be to note trends and developments, recognise how they are related, and think them through from the perspective of iGovernment, i.e. beyond the boundaries of ministries and levels of government, and with a view to potential future developments. The committee's advice would focus specifically on the 'warning flags' described above, i.e. networked information, composite information, and preventive and pro-active policy. Its annual report would be made available in the public domain and offer information-related (as opposed to technology-related) recommendations relating to government's plans, viewed within the broader context of iGovernment and iSociety. Where relevant, its advice would specifically consider European and international trends and developments. Decisions taken at these levels often only emerge as topics of political and social debate in the Netherlands at a much later stage. Because they influence how iGovernment and its branches beyond the Dutch borders develop, however, they should be noted, discussed and thought through at a more appropriate point in time.

The committee's agenda must involve more than just advising on planned measures, however. One recurring item would be to evaluate ICT projects – whether up and running, abandoned, or completed – in the light of information flows and the relationship between service, care and control. The very fact that iGovernment consists of ongoing processes of linking and diversification makes it crucial to keep close track of projects and links, draw lessons from the past, and encourage the relevant debate. Ideally, that debate should concern function creep and similar matters, with function creep being recognised both as an inherent feature of innovation and as a problem – i.e. opposite sides of a coin that can be confusingly similar at times. Drawing on the annual reports of the iPlatform and iAuthority (see below), the committee would also take stock of situations and systems in which citizens (and companies) have run into difficulties and, at a more general level, draw lessons from such cases and monitor them for improvement or deterioration. One specific point to watch for would be the all-too-common tendency to evaluate ICT projects strictly from the narrow perspective of the technology or the budget involved. The committee must focus much more explicitly on facilitating and carrying out evaluations that consider whether the new application in fact delivers the information specified by the underlying policy objective. If the aim is to embed 'iGovernment self-awareness' throughout government, then a willingness to learn is more important – at least for the time being – than any accountability mechanisms.

The committee's report would be discussed in both chambers of Parliament and in the presence of the committee's chairperson. It would be up to the House of Representatives to draw conclusions from the recommendations. The Coordinat-

ing CIO would run the committee's secretariat, as this would create an institutional relationship between iGovernment self-awareness in the Government and in Parliament. The new task would also boost the strategic position of the Coordinating CIO and improve his or her forward-looking capacity.

The Office of the Coordinating CIO could help establish a broad public forum to support and assist the committee. The forum, an advisory body, would nurture the relationship between the permanent committee for iGovernment and the iSociety. Following the example of the broadly-based Standardisation Forum – set up to support the Standardisation Board – the iGovernment forum would provide the permanent committee with ideas, express its concerns, and suggest solutions. The forum would be made up of a wide range of stakeholders and experts. In addition to representatives of ministries, government agencies and local authorities, it would also include experts from the private sector (not representing specific businesses but based on the particular expertise that they can bring to the table), scientists, supervisory bodies, and 'citizens', i.e. NGOs such as the Consumers' Association and human rights organisations. In 2001, the Docters van Leeuwen Committee suggested setting up a similar body (which it called the 'Platform for the Electronic Society') to advise a government commissioner (ICT and Government Ad Hoc Advisory Committee 2001). At the time, the Government rejected this proposal, pointing out that the Minister for Urban Policy and Integration played a coordinating role with respect to ICT. In its official comments, the Government concluded that the Minister would provide a more effective institutional anchor. But that argument no longer holds water. iGovernment represents a break with government's tradition of thinking in terms of eGovernment; the approach it requires differs from the role that a coordinating minister can or may even want to play. The networks that make up iGovernment, whether internal or external, and recognition of their impact make for an agenda that should not be restricted to a single ministry or even exclusively to government. iGovernment will become a matter of coordination only when self-awareness of iGovernment has been well and truly embedded throughout the system.

9.3.2 IPLATFORM AND IAUTHORITY

There is strong evidence that an enormous 'back office' of government information flows has been created, which sometimes extends beyond the boundaries of government. As mentioned above, much of the information in these networks has been 'abandoned', in the sense that no one claims responsibility for it. It is sometimes impossible for citizens to correct erroneous information, even though they are confronted with the consequences of such errors in their dealings with government. In addition to the extreme cases of identity fraud that make the headlines, there are numerous other situations in which citizens have attempted to correct contaminated government information but did not know where to turn. The

organisations that should be there to assist these citizens are limited in scope and ill-equipped for their task: some are only temporary; others do not deal with individual cases; many of them operate with barebones staff and funding; and none of them is empowered to take binding decisions that will actually correct errors in the underlying network. Even the Office of the National Ombudsman, after reviewing the most publicised case of identity fraud (the Kowsoleaa case), had to admit the impossibility of correcting erroneous information once and for all.

But the 'abandonment' issue goes beyond erroneous information alone. It also applies to the information that government communicates to citizens through a patchwork of websites, e-helpdesks and Web portals. A growing number of these projects involve multiple parties (including private-sector actors) and have arisen without the benefit of democratic legitimacy or decision-making. In many of these new networked communication models, and in the communication that takes place through them, there is no clear allocation of official responsibility for the information made available. The societal function can be implemented by properly organising transparency and accountability in a way that protects citizens against falling victim to those elements of iGovernment that they can neither fathom nor influence.

iGovernment transparency and accountability must have an identifiable 'home'. Citizens should have access to a single platform that concerns itself with transparency and a single authority that is responsible for accountability.

In the same way that government is attempting to provide its service through a single helpdesk, it should also consider concentrating responsibility for transparency and data correction in a single access point or portal. That would mean clustering government forums that are currently dispersed over different websites and that tend to be application or problem-driven[5] at a single digital location. The iGovernment Platform would serve as an interactive source of information about the use of ICT in the relationship between government and the citizen. To increase transparency it would clarify to citizens what kinds of records are held on them in the linked systems of iGovernment, who has access to those records, and why – and provide that information through a clear and unambiguous information portal. Following the example of the Tax and Customs Administration's allowances portal, such a Platform would allow citizens to alter and correct their personal data themselves within a secure environment, and it would also guarantee that those alterations will then be implemented throughout the entire network. Making the transparency function interactive would also empower citizens. Adding interactivity to the platform would reflect a broader tendency in iSociety, with digitization improving and driving the potential for citizen empowerment.

The second societal function, accountability, is active and has already been advocated by the National Ombudsman (2009). The iAuthority must ensure that any misrepresentation of citizens in the back office or other systems is actually corrected. Citizens must literally be relieved of the burden of rectifying and solving problems that creep into the chains and networks of iGovernment. This proposal represents a radical centralisation of accountability. The existing procedures and methods – whereby errors that have crept into the network must be corrected locally and via different institutions and supervisory bodies – have proved to be inadequate. The new iAuthority must combine expertise and a personal approach with the power to take binding decisions *vis-à-vis* the organisations that populate the back-office network of iGovernment. It is very important that the iAuthority should in fact possess such authority; if it does not, it will be given the same run-around as the hapless citizen, and the problem would simply be shifted on to another's shoulders rather than resolved. Careful thought must also be given to the degree of access that the citizen should have to the iAuthority. On the one hand, it should be a recognisable and low-threshold institution; on the other, too low a threshold makes it all too easy for certain individuals to throw a spanner into the works of iGovernment,[6] given the amount of effort that the model requires on the part of the administrators.

The iPlatform could act as a digital extension of the current government portal mijnoverheid.nl (mygovernment.nl). In organisational terms, the iAuthority should be set up as an autonomous body with the power to take binding decisions. All existing information platforms and operational organisations (including the Identity Fraud Helpdesk), should be merged into or combined within these organisations. The iPlatform and the iAuthority would publish a combined annual report describing their work and the results they had attained and reviewing the most important trends and developments of the past year.

9.3.3 PROFESSIONALISING COMMISSIONING PRACTICES

Ultimately, iGovernment self-awareness must also be extended to the technical realm, i.e. with respect to the development of standards, applications, and links between data and information flows. This is the operational function. It is, after all, the engineers and systems designers and the relevant national and international bodies that determine what iGovernment will look like at the operational level. The realisation that the relevant decisions are essentially political or policy-driven is often cancelled out by the notion that technology is nothing more than an instrument. Anyone who follows the flow of information – as we have done in this book – knows that technology gives rise to categories and that 'categories have politics.' That means that questions of design, standardisation and interoperability are all decisive for the way iGovernment develops as a whole, and not just for individual applications and decisions. One of the critical elements in the evolu-

tion of iGovernment is the quality of government commissioning practices in the field of ICT. By specifying the requirements for a new system or application and identifying what functions it must have, government is in fact setting the stage for future applications and how they fit into the broader context of iGovernment. Government faces a dilemma in that respect: on the one hand, it wants to be in charge of development, for example via the ICTU; on the other, it is impossible and impractical for government itself to have all the necessary technical knowledge in house. Most of the technical specialists who 'work for government' are in fact external consultants and experts. The result is over-investment in technical know-how and too little concern for the interaction between policy, implementation, and technology in information flows.

Government's commissioning practices must therefore be remodelled: instead of investing in technical expertise, it should invest in knowledge at the interface of policy, implementation, and technology. If it aims to take systematic action to solve ICT problems, then it will have to turn its attention from technical development to professional outsourcing. That means that the technical side of things must be left largely in the hands of parties that operate outside government (by contracting these external parties to develop applications or by purchasing applications in the commercial marketplace). Instead, government should learn how to frame an assignment; accurately define the specifications, legal context and underlying conditions; place the assignment in a broader context; and provide professional supervision during development. It is up to the developer to ensure that the technology actually works, but it the commissioning party's job to ensure (by supervising and guiding the work) that the technology generates the 'right' information and facilitates information processes that fit in well with the relevant policy and with the wishes of the agencies or other organisations that will actually implement it. This means setting up an organisation that is responsible for government commissioning practices and that is not limited by the boundaries between ministries and individual agencies. Such an organisation would employ a small group of 'core' ICT specialists and legal experts in ICT matters who understand iGovernment. That core group would be joined, on a project-by-project basis, by the CIO and other officials from the relevant ministry, and by the agency staff who will ultimately have to work with the system. It would seem obvious that the partners in the chain or network should always be involved in developing a new system or application, but in fact this rarely ever happens. Here too, the information flows generally outstrip the relevant organisations.

iGovernment must improve its commissioning practices by investing in knowledge at the interface of policy, implementation, and technology, rather than by investing purely in in-house technical expertise and development capacity.

9.4 IMPLEMENTING IGOVERNMENT

If the Dutch Government is to take on board the reality of iGovernment and become capable of prudently guiding its development, it must make the transition from eGovernment to iGovernment in thought, word and deed. For government to tread the path of digitization with confidence, iGovernment self-awareness will need to be embedded at every level. Government faces a crucial challenge in that respect: it must be willing and able to move the focus of debate from technology and individual applications to a new level, i.e. to interrelated information processes and linked information. What is essential is to create enough leeway and generate enough interest in weighing up the driving, underpinning and process-based principles and to do so with an open mind. Scrupulous development of iGovernment cannot proceed without such an assessment, and it is vitally important to consider iGovernment as a whole. In addition, government must exercise particular caution, both in this assessment and in its policymaking and policy implementation, whenever the three processes of information handling noted in this book come into play. These processes – furnished with symbolic warning flags – are associated with a) the networking of information, b) the compiling and enhancing of information, and c) the pursuit of preventive policy based on information. The specific implications that these processes have for policy implementation, the position of the citizen, the quality of government information management, and the internal and external reference points for liability and accountability make it vital to look critically at the usefulness, necessity, and impact on society of digitization projects.

To support government as it meets this challenge and ensure the necessary institutional grounding, this book lays out an agenda for institutional transformation. The institutions proposed within the context of this transition are intended to guarantee that iGovernment is equipped with the tools it needs to foster self-awareness, protection, and innovation. It must be clear that the institutional transformation as such is much more important than the specific form and nametags of the institutions proposed in this volume. The transition will need to take place at three different levels: the strategic level (by installing a permanent committee for iGovernment), the societal level (via an iPlatform responsible for transparency and an iAuthority responsible for accountability), and the operational level (by instilling professional commissioning practices in government and prioritising knowledge at the interface of technology and policy above technical know-how). Finally, in the case of both the challenge that government faces and the necessary institutional transformation, the development of iGovernment cannot be viewed as separate from the path that the iSociety as a whole is treading.

NOTES

1 That is ultimately also a collective interest, because a society that does not forgive and forget is a fundamentally different society to one in which people are permitted to start again.

2 In a statement, Senator Joseph Lieberman said that providers such as Amazon (which had hosted WikiLeaks) should cut all ties with WikiLeaks. "I will be asking Amazon about the extent of its relationship with WikiLeaks and what it and other web service providers will do in the future to ensure that their services are not used to distribute stolen, classified information"; see "Banishing WikiLeaks" by Amy Davidson in *The New Yorker*, www.newyorker.com/online/blogs/closeread/2010/12/banishing-wikileaks. html#ixzz174 SMOBQA, requested on 10 December 2010.

3 Interview with Peter Wijntje and Sjoerd Peereboom (Ministry of Finance/Tax and Customs Administration), 19 October 2010.

4 LJN: BK6331, Dutch Supreme Court, 08/04524 B.

5 Examples include burgerservicenummer.nl (for the BSN), infobsnzorg.nl (for the EPD), lastvandeoverheid.nl, mijnoverheid.nl, and the Identity Fraud Helpdesk for the public.

6 Cf. discussions on (among other things) environmental organisations and their sometimes disruptive access to the administrative courts.

AFTERWORD: iGOVERNMENT AND iSOCIETY

In essence, this publication is about government taking responsibility for the way it uses ICT. The role that government plays in the information society and the responsibility that it bears go much further, however. In addition to being accountable for iGovernment, government is also responsible, to a certain extent, for the way the iSociety as a whole functions. Such sweeping responsibility can be defined in terms of the following questions: What aspects of the information society should government be concerned about? Should it intervene? If so, how? Former Dutch Prime Minister Wim Kok addressed this issue in April 2001 at the Infodrome Conference: "We must nevertheless ask ourselves what responsibilities government will face in the years ahead in connection with the consequences inherent to the information society." That responsibility can be described as the system responsibility that iGovernment has for the iSociety. Any intervention in the iSociety will naturally be politically charged and to a certain extent controversial, but an attempt must nevertheless be made to find common ground for matters that government is obliged to guarantee. iGovernment's system responsibility cannot simply be ignored.

That is because, first of all, government must stand up for its citizens when the private sector fails to adequately guarantee their interests. For example, the growing power over information exercised by such global corporations as Google, Facebook and Apple will force government (and the European Union) to consider whether – and if so how – that power should be restricted in the public interest. There have already been certain moves in that direction. Responding to questions raised by Parliament in August 2010, the then Minister of Economic Affairs Maria van der Hoeven undertook to ask the Data Protection Authority (CBP) to evaluate a new clause in Apple's privacy policy.[1] In some cases, questions touching on government's system responsibility will need to be addressed at the European level and through a European actor (a 'lead authority'[2]) because it is only the European Union that has the necessary weight and authority to take forceful action. However, the popularity of interactive communication in social networks and through Web 2.0 raises another question: is it government's responsibility to control or restrict the behaviour of citizens and/or to protect them against commercial actors in that sphere? To a certain extent, moreover, government's system responsibility in these and other cases can be legally enforced as a human rights matter (De Hert 2011).

"It is not true that European jurisprudence offers the authorities too little in the way of specific guidelines. The Court of Justice has formulated general principles concerning the protection of personal data that are being applied in a growing number of cases. The same is true, to a somewhat lesser extent, of the battle against identity fraud and the protection of media pluralism. The Netherlands can make good use of these principles" (De Hert 2011).

How iGovernment should interpret its system responsibility is in our view, the key issue – we've moved beyond the question as to whether it should do so at all.

Secondly, system responsibility becomes an issue when trends in the private sector interfere too blatantly with crucial government policy. Cases in point are the various advances in the area of identity management. As we saw in Part II, government is making a major investment in digital identity tools, for example the biometric passport, the DigiD system, and (potentially) the eLicence. It is precisely because it is investing heavily in identity authentication – and makes claims as to its accuracy – that government must also concern itself with identity authentication in the semi-public and commercial sectors, in particular where there is a risk that the quality will deteriorate. What is the point of investing in the data security of a national database under the terms of the Passport Act, when the same data is also generally available beyond the domain of government? The introduction of the biometric passport raises questions about the use of biometrics in the private sector. Little has been done to regulate such use, and politicians have so far ignored this issue. Swimming pools, supermarkets, employers and computer manufacturers, for example, will be at liberty to experiment with new applications.

The growing stockpile of information also makes identification an increasingly important key for linking and combining data outside the context of government. Experience shows that the use of digital identities is blurring the boundaries between the public and private sectors. The impact of that use is therefore spilling over the same boundaries, especially when private-sector actors have duties under public law (civil-law notaries) or when government requires private actors to establish the identity of individuals – under the Compulsory Identification Act (*Wet identificatieplicht*; provision of services; employment) – based on the identity documents issued by government. For example, the BSN was conceived as an identity authentication code for government services; no one considered the possibility that it would very quickly catch on as a universal (public-private) unique identifier. For these and other reasons, government must keep a careful eye on trends outside its own territory and consider whether and when stricter guidelines or rules are required.

The fact that government bears final responsibility in such cases does not mean that it must take matters solely into its own hands (De Hert 2011) or even that it has the capacity or leeway in its own organisation to do so (Meijer 2011). There are, however, a number of pitfalls that it must try to avoid with regard to this fundamental responsibility. First of all, ministers must think hard before deciding to intervene. Government naturally has a duty to intercede in societal relationships (in this case informational relationships): that is one of its *raisons d'etre*. At the same time, however, such intervention can be risky: it can be thwarted by social dynamics for all kinds of reasons, and government must anticipate such a possibility. Secondly, it would be risky to adopt an 'ICT user's mentality' at the start of an intervention. The information society – the ICT-immersion of everyday life – does not 'belong' to government in the way that its own ICT systems do, and government must be aware that there are constitutional aspects that need to be taken into account when it decides to intervene. Thirdly, there are different ways to intervene, and it is all too easy to choose the wrong one. To start with the most traditional scenario: government can decide to intervene in informational relations by imposing mandatory regulations. It can also take a 'soft' approach, however, and merely offer itself as an interlocutor for private players. The middle ground between the two extremes is facilitatory: it can create the right basic conditions for society to work out its own potential solutions. Each of these *modi operandi* is based on a different conception of responsibility.

According to Meijer (2011), however, it is becoming more difficult, and indeed perhaps impossible, for government – as the actor bearing system responsibility – to play a key role in the turbulence and complexity of technological networks. "Instead of overall responsibility, government can increasingly claim two other responsibilities: procedural responsibility and miscellaneous responsibility." Procedural responsibility means that government would no longer be responsible for outcomes, but merely for the quality of the process. Miscellaneous responsibility would allow government to guarantee that those involved are making an effort to protect citizens and prevent system failures. It would involve government taking on the duties that others have failed to fulfil. The permanent committee for iGovernment proposed above could play an important role in setting the agenda for the concept of government system responsibility. The key questions that the committee would address are: what trends and developments in the broader iSociety should be encouraged or discouraged, and what is the most suitable level for taking regulatory action (national or international)? Which general trends and developments can be expected to trickle down to iGovernment and what does that imply for any regulatory action?

However, certain iSociety trends will increasingly force government to face fundamental questions that it has not even begun to answer. The speed at which information is disseminated and copied – even (or especially) when it is unwel-

come to government – means that the authorities will also have to consider their own information management system. The WikiLeaks affair has made that patently clear. Transparency is generally regarded as something that government concedes to citizens (passive transparency); it is not often considered a virtue worth practising (active transparency), and certainly not something that only a handful of citizens can claim or force from government. In today's digital world, however, the authorities will increasingly have to consider precisely how they intend to deal with transparency. As John Naughton commented in *The Guardian*, the authorities must "[l]ive with the WikiLeakable world or shut down the net. It's [their] choice" (Naughton 2010b). They are not likely to choose the latter option. Nevertheless, they will need to find a new balance between freedom of the press, data confidentiality and data security; a regulatory system may be an option. Part of the answer may lie in regulating parties outside government (servers, clouds etc.), but part of it may also require government to engage in self-examination. Some information should perhaps not be stored at all; other information sources should be more transparent rather than confidential and secret; and still other information should be stored more securely than it currently is.[3] But government can never entirely rule out the unpredictability and uncertainty of society and, consequently, the iSociety.

When it comes to iGovernment's responsibility for the iSociety, the frame of reference is the same as when assessing government's use of ICT. In essence, we can define government's system responsibility by – once again – weighing up the driving, underpinning and process-based principles, although in this case the driving principles often operate beyond the boundaries of government. The public and businesses move ahead, inspired by the promise of new technologies and profits. When this drive is not offset against underpinning principles or kept in check by the process-based principles that make information flows transparent for the public and – if necessary, open to criticism – then those responsible for iGovernment should at the very least ask themselves whether the time has not come to take action.

NOTES

1 Memorandum by the Minister of Economic Affairs responding to questions about a new clause in Apple's privacy conditions, 3 August 2010.

2 There are now arguments within the EU in favour of a "lead authority" with sufficient powers to resolve these sorts of issues for the 27 Member States (interview with J. Hennis-Plasschaert, Liberal Party (VVD). Formerly MEP, now MP in the Dutch House of Representatives, 4 November 2010).

3 As suggested by Bits of Freedom (among others) in its analysis of the WikiLeaks 'Cablegate affair'. See Ot van Daalen, *De wereld na Wikileaks' Cablegate*, at www.bof.nl/2010/12/10/de-wereld-na-wikileaks-cablegate.

ABBREVIATIONS AND ACRONYMS

ACTA	Anti-Counterfeiting Trade Agreement
AIVD	*Algemene Inlichtingen- en Veiligheidsdienst* / General Intelligence and Security Service
ANPR	Automatic Number Plate Recognition
ANWB	*Algemene Nederlandse Wielrijders Bond* / Royal Dutch Touring Club
AWBZ	*Algemene Wet Bijzondere Ziektekosten* / Exceptional Medical Expenses Act
BKWI	*Bureau Keteninformatisering Werk en Inkomen* / Work and Income Chain Computerisation Office
BPR	*Agentschap Basisadministratie Persoonsgegevens en Reisdocumenten* / Personal Records Database and Travel Documents Agency
BSN	*Burgerservicenummer* / Citizen Service Number
CBP	*College Bescherming Persoonsgegevens* / Data Protection Authority
CBR	*Centraal Bureau Rijvaardigheidsbewijzen* / Central Office for Motor Vehicle Driver Testing
CBS	*Centraal Bureau voor de Statistiek* / Statistics Netherlands
CIO	Chief Information Officer
CIOT	*Centraal Informatiepunt Onderzoek Telecommunicatie* / Central Information Point for Telecommunications Investigation
CIZ	*Centrum Indicatiestelling Zorg* / Care Needs Assessment Centre
CJIB	*Centraal Justitieel Incassobureau* / Central Fine Collection Agency
CVZ	*College voor Zorgverzekeringen* / Health Care Insurance Board
CWI	*Centrum voor Werk en Inkomen* / Centre for Work and Income
ECHR	European Court of Human Rights
ECP-EPN	Platform for the Information Society
ECPHR	European Convention for the Protection of Human Rights and Fundamental Freedoms
EDPS	European Data Protection Supervisor
EKD	*Elektronisch Kinddossier* / Electronic Child Dossier
EMD	*Elektronisch Medisch Dossier* / Electronic Medical Dossier
EPD	*Elektronisch Patiënten Dossier* / Electronic Patient Dossier
EUR	*Erasmus Universiteit Rotterdam* / Erasmus University Rotterdam
FCC	Federal Communications Commission
GBA	*Gemeentelijke Basisadministratie* / Municipal Personal Records Database
GDP	Gross Domestic Product
GPS	Global Positioning System
GSD	*Gemeentelijke Sociale Dienst* / Municipal Social Services
HARM	Hospital Admissions Related to Medication
HEC	*Het Expertise Centrum* / The Expertise Centre
HKS	*HerKenningsdienst Systeem* / ReCognition System
ICAO	International Civil Aviation Organization

ICTU	*ICT Uitvoeringsorganisatie* / Netherlands ICT Implementation Organisation
IMI	Internal Market Information system
IND	*Immigratie- en Naturalisatiedienst* / Immigration and Naturalisation Service
ISP	Internet Service Provider
KLPD	*Korps landelijke politiediensten* / National Police Service Agency
LIS	*Landelijk Informatiesysteem Schulden* / National Debt Information System
MI5	Military Intelligence, Section 5 (UK)
NORA	*Nederlandse Overheids Referentie Architectuur* / Dutch Government Reference Architecture
NUP	*Nationaal uitvoeringsprogramma betere dienstverlening en e-overheid* / National Implementation Programme on Service Delivery and eGovernment
OECD	Organisation for Economic Co-operation and Development
PET	Privacy Enhancing Technologies
PNR	Passenger Name Records
R&D	Research and Development
RAND	Research and Development Corporation
RDW	*Rijksdienst voor het Wegverkeer* / Centre for Vehicle Technology
RFID	Radio-Frequency Identification
RINIS	*Routerings Instituut voor (inter)Nationale Informatiestromen* / Institute for the Routing of (Inter)National Information Streams
SCP	*Sociaal en Cultureel Planbureau* / Netherlands Institute for Social Research
SIOD	*Sociale Inlichtingen- en Opsporingsdienst* / Social Intelligence and Investigation Service
SIS	Schengen Information System
SISA	*Stadsregionaal Instrument Sluitende Aanpak* / City-wide and Regional Instrument (Comprehensive Network)
SUWI	*Structuur Uitvoeringsorganisatie Werk en Inkomen* / Work and Income Implementation Structure
SVB	*Sociale Verzekeringsbank* / Social Insurance Bank
SWIFT	Society for Worldwide Interbank Financial Telecommunication
UWV	*Uitvoeringsinstituut Werknemersverzekeringen* / Social Security Agency
VIPS	*Versterking Identiteitsketen Publieke Sector* / Reinforcement of Public Sector Identity Chain
VIR	*Verwijsindex Risicojongeren* / Reference Index for Juveniles at Risk
VNG	*Vereniging Nederlandse Gemeenten* / Association of Dutch Municipalities
WAJONG	*Wet arbeidsongeschiktheidsvoorziening jonggehandicapten* / Invalidity Insurance (Young Disabled Persons) Act
WIA	*Wet werk en inkomen naar arbeidsvermogen* / Work and Income (Fitness for Work) Act
WOB	*Wet Openbaarheid van Bestuur* / Government Information (Public Access) Act
WSW	*Wet sociale werkvoorziening* / Sheltered Employment Act

REFERENCES

ACTAL (2010) *Brief van 10 mei 2010 Advies ICT-beleid en vermindering regeldruk* (for ICT research: *Uit het Zicht. Beleidsmaatregelen voor het versnellen van het gebruik van ICT-toepassingen voor administratieve lastenverlichting)*, The Hague.

Adviescommissie Informatiestromen veiligheid (2007) *Data voor daadkracht. Gegevensbestanden voor veiligheid: observaties en analyse*, April 2007, The Hague: Deltahage.

Akker, R. van den & M. Kuiper (2008) 'De bureaucraat als dompteur. De domesticatie van de digitale overheid', pp. 153-165 in V. Frissen & J. de Mul (eds.) *De Draagbare Lichtheid van het Bestaan*, Kampen: Uitgeverij Klement.

Algemene Inlichtingen- en Veiligheidsdienst (2010a) *Jaarverslag 2009*, The Hague: Ministerie van Binnenlandse Zaken en Koninkrijksrelaties.

Algemene Inlichtingen- en Veiligheidsdienst (2010b) *Kwetsbaarheidsanalyse spionage*, The Hague: AIVD.

Algemene Rekenkamer (1991) *Machineleesbare gegevens. Archivering en beheer bij het Rijk*, The Hague: SDU.

Algemene Rekenkamer (1998) *Beheer en archivering van digitale bestanden*. Kamerstukken II 1997-1998, 25970, no. 2.

Algemene Rekenkamer (2003) *Communicatienetwerk C2000 en Geïntegreerd Meldkamersysteem (GMS)*, The Hague: SDU.

Algemene Rekenkamer (2007a) *Lessen uit ICT-projecten bij de overheid*, The Hague: SDU.

Algemene Rekenkamer (2007b) *Aanbesteding ICT-Component P-Direkt*, The Hague: SDU.

Algemene Rekenkamer (2008a) *Lessen uit ICT-projecten bij de overheid - part B*, The Hague: SDU.

Algemene Rekenkamer (2008b) *ICT-project huur- en zorgtoeslag*, The Hague: SDU.

Algemene Rekenkamer (2009) *Informatiehuishouding van het Rijk*, The Hague: SDU.

Algemene Rekenkamer (2010a) *Informatiehuishouding van het Rijk. Overzicht van een dynamisch vraagstuk, een achtergrondstudie,* The Hague: SDU.

Algemene Rekenkamer (2010b) *Informatiehuishouding van het Rijk, Stand van zaken juni 2010 fact sheet*, www.rekenkamer.nl/Actueel/Onderzoeksrapporten/Bronnen/2010/06/Factsheets_Vooropname/Informatiehuishouding_van_het_Rijk, consulted on 24 September 2010.

Allen, A. (2003) *Why Privacy Isn't Everything: Feminist Reflections on Personal Accountability*, Lanham, MD: Rowman and Littlefield.

Ambtelijke Commissie Toezicht II (2004) *Rapport van Bevindingen betreffende de zelfevaluatie door het College Bescherming Persoonsgegevens (CBP) van het toezicht op de verwerking van persoonsgegevens*, (The Hague, 16 December 2004).

Anders, G. (1980) *Die Antiquiertheit des Menschen. Über die Seele im Zeitalter der zweiten industriellen Revolution*, Munich: C.H. Beck.

Anderson, C. & M. Wollf (2010) 'The Web Is Dead. Long Live the Internet', *Wired Magazine*, September 2010, www.wired.com/magazine/2010/08/ff_webrip/.

Andeweg, R. & H. van Gunsteren (1994) *Het grote ongenoegen: over de kloof tussen burgers en politiek*, Haarlem: Aramith.

Arendt, H. (1998) *The Human Condition*, 2nd edition. Chicago: University of Chicago Press.

Article 29 Data Protection Working Party and Working Party on Police and Justice (2009) *The Future of Privacy*, Joint Contribution to the Consultation of the European Commission on the Legal Framework for the Fundamental Right to Protection of Personal Data, 02356/09/EN, WP 168.

Attema, J. & D. de Nood (2010) *Over de rolverdeling tussen overheid en burger bij het beschermen van identiteit*, report of ECP-EPN in cooperation with the WRR, WRR webpublication nr.47, www.wrr.nl.

Aus, J. (2008) *EU Governance in an Area of Freedom, Security and Justice. Logics of Decision Making in the Justice and Home Affairs Council*. Dissertation: University of Oslo.

Baker, S. (2008) *The Numerati*, Boston: Houghton Mifflin.

Balzacq, T. (2008) 'The Policy Tools of Securitization. Exchange, EU Foreign and Interior Policies', *Journal of Common Market Studies* 46, 1: 75-100.

Barney, D. (2004) *The Network Society*, Cambridge: Polity.

Beck, U. (1992) *Risk Society. Towards a New Modernity*, London: Sage Publications.

Bekkers,V.J.J.M. (1998) *Grenzeloze overheid. Over informatisering en grensveranderingen in het openbaar bestuur*, Alphen aan den Rijn: Samsom.

Bekkers, V.J.J.M. & S. Zouridis (1999) 'Electronic Service Delivery in Public Administration: Some Trends and Issues', *International Review of Administrative Sciences* 65: 183-195.

Bekkers, V.J.J.M. (2000) *Voorbij de virtuele organisatie? Over de bestuurskundige betekenis van virtuele variëteit, contingentie en parallel organiseren*, The Hague: Elsevier.

Bekkers, V.J.J.M. (2001) De mythen van de elektronische overheid. Over retoriek en realiteit, *Bestuurswetenschappen* 4: 277-295.

Bekkers, V.J.J.M. & M. Thaens (2002) 'EGovernment op een kruispunt van wegen', *Bestuurskunde* 8: 328-337.

Bekkers, V., M. Lips & A. Zuurmond (2005) 'De januskop van ICT in het publieke domein', pp. 733-752 in M. Lips et al. (ed.) *ICT en openbaar bestuur. Implicaties en uitdagingen van technologische toepassingen voor de overheid*, Utrecht: Lemma.

Bekkers, V. & M. Thaens (2005) 'Sturing, informatie en ICT', pp. 137-160 in M. Lips et al. (ed.) *ICT en openbaar bestuur. Implicaties en uitdagingen van technologische toepassingen voor de overheid*, Utrecht: Lemma.

Bekkers, V., H. van Duivenboden & M. Lips (2005) 'ICT en publieke dienstverlening', pp. 237-256 in M. Lips et al. (ed.) *ICT en openbaar bestuur. Implicaties en uitdagingen van technologische toepassingen voor de overheid,* Utrecht: Lemma.

Bekkers, V.J.J.M. & V. Homburg (2009) 'The Myths and Ceremonies of eGovernment: beyond the Hype of a New and Better Government?', pp. 217-234 in A. Meijer et al. (ed.) *ICTs, Citizens and Governance: after the Hype*, Amsterdam: IOS Press.

Bekkers, V.J.J.M. & A. Meijer (2010) *Cocreatie in de publieke sector. Een verkennend onderzoek naar nieuwe, digitale verbindingen tussen overhead en burger*, The Hague: Boom Juridische Uitgevers.

Bemt, P. van den (2006) *HARM (Hospital Admissions Related to Medication*), Utrecht: Universiteit van Utrecht.

Bennett, C. J. (2008) *The Privacy Advocates: Resisting the Spread of Surveillance,* Cambridge MA: MIT Press 2008.

Bennett, C., C. Raab & P. Regan (2003) 'People and place. Patterns of individual identification within intelligent transportation systems', pp. 153-175 in D. Lyon (ed.) *Surveillance as Social Sorting. Privacy, Risk and Digital Discrimination*, London: Routledge.

Berg, B. van den (2008) 'Ik doe er niet aan mee. Niet-gebruikers in een technologische wereld', pp. 263-280 in M. van den Berg, C. Prins & M. Ham (eds.) *In de greep van de technologie. Nieuwe toepassingen en het gedrag van de burger*, Amsterdam: Van Gennep.

Berg, B. van den (2009) 'Slijp de messen', *Flux september 2009*, The Hague: Rathenau Institute.

Berg, B. van den & R.E. Leenes (2011) 'Keeping up Appearances: Audience Segregation in Social Network Sites' in P. de Hert (ed.) *Computers, Privacy and Data Protection: An Element of Choice,* Dordrecht: Springer.

Berg, M. van den, C. Prins & M. Ham (2008) *In de greep van de technologie. Nieuwe toepassingen en het gedrag van de burger*, Amsterdam: Van Gennep.

Berkvens, J.A. (1992) 'Van Heerendiensten naar Informatiediensten', pp. 109-130 in P.H.A. Frissen et al. (ed.) *Orwell of Athene Democratie en Informatiesamenleving,* The Hague: Sdu.

Besters, M. (2010) 'De schaduwzijden van het Schengen Informatie Systeem', pp. 74-85 in G. Munnichs et al. (ed.) *Databases. Over ICT-beloftes, informatiehonger en digitale autonomie*, The Hague: Rathenau Institute.

Besters, M. & F. Brom (2010) 'Greedy Information Technology: The Digitalization of the European Migration Policy', *European Journal of Migration and Law* 12: 455-470.

Bijker, W. & J. Law (eds.) (1992) *Shaping Technology/Building Society. Studies in Sociotechnical Change,* Cambridge, MA: MIT Press.

Bijker, W. (2001) 'Understanding Technological Culture through a Constructivist View of Science, Technology, and Society', pp. 19-34 in S. Cutcliffe & C. Mitcham (eds.) *Visions of STS: Counterpoints in Science, Technology, and Society Studies*, New York: State University of New York Press.

Biometric Technology Today (2009) 'Biometrics Review: 2008/2009', *Biometric Technology Today,* January 2009: 9-11.

Blok, P. (2002) *Het recht op privacy. Een onderzoek naar de betekenis van het begrip 'privacy' in het Nederlandse en Amerikaanse recht*, The Hague: Boom Juridische Uitgevers.

Boersma, K., A. Meijer & P. Wagenaar (2009) 'Unraveling and Understanding the eGovernment Hype', pp. 217-234 in A. Meijer et al. (ed.) *ICTs, Citizens and Governance: after the Hype*, IOS Press.

Böhre, V. (2010) *Happy landings? Het biometrische paspoort als zwarte doos*, WRR webpublication nr. 46, www.wrr.nl.

Bonthuis, M.J. & J. Holvast (2010) *Blackbox-onderzoek Veiligheidshuizen*, WRR web publication nr. 49, www.wrr.nl.

Borking, J.J.F.M. (2010) *Privacyrecht is Code, Over het gebruik van Privacy Enhancing Technologies*, dissertation, Leiden.

Borst, W.L. (2009) *Jegens en Wegens. Over persoonsgebonden informatie in de strafrechtsketen*, Nijmegen: Wolf Legal Publishers.

Boschker, E., P. Castenmiller & A. Zuurmond (2010) 'Dynamiek in de gemeentelijke basisadministratie', pp. 86-98 in G. Munnichs et al. (eds.) *Databases. Over ICT-beloftes, informatiehonger en digitale autonomie*, The Hague: Rathenau Institute.

Boswell, C. (2007) 'Migration Control in Europe after 9/11: Explaining the Absence of Securitization', *Journal of Common Market Studies* 45, 3: 589-610.

Boutellier, H. (2004) *The Safety Utopia: Contemporary Discontent and Desire as to Crime and Punishment.* Dordrecht: Kluwer Academic Publishers.

Boutellier, J.C.J. (2007) *Nodale orde: Veiligheid en burgerschap in een Netwerksamenleving*, oration Free University, Amsterdam.

Bovens, M. & S. Zouridis (2002) 'From Street-Level to System-Level Bureaucracies: How Information and Communication Technology is Transforming Administrative Discretion and Constitutional Control', *Public Administration Review* 62, 2: 174-184.

Bovens, M. (2003) *De digitale republiek. Democratie en rechtsstaat in de informatiemaatschappij*, Amsterdam: Amsterdam University Press.

Boyd, D. (2008) *Taken out of Context: American Teen Sociality in Networked Publics***.** PhD Dissertation. University of California-Berkeley, School of Information.

Broeders, D. (2007) 'The New Digital Borders of Europe. EU Databases and the Surveillance of Irregular Migrants', *International Sociology* 22, 1: 71-92.

Broeders, D. (2009) *Breaking down Anonymity. Digital Surveillance of Irregular Migrants in Germany and the Netherlands.* Amsterdam: Amsterdam University Press.

Broeders, D. (2011) 'Grensoverschrijdende mobiliteit van personen en de digitale grenzen van Europa' in D. Broeders, C. Cuijpers & J.E.J. Prins, *De staat van informatie*, WRR verkenning nr. 25, Amsterdam: Amsterdam University Press.

Broeders, D. (2011b) 'A 'European Border' Surveillance System under Construction', pp. 40-67 in H. Dijstelbloem & A. Meijer (eds.) *Migration and the New Technological Borders of Europe.* Houndsmills, Basingstoke and Hampshire: Palgrave.

Broeders, D., C. Cuijpers & J.E.J. Prins (ed.) (2011) *De staat van informatie*, WRR verkenning nr. 25, Amsterdam: Amsterdam University Press.

Brouwer, E. (2008) *Digital Borders and Real Rights. Effective Remedies for Third-Country Nationals in the Schengen Information System*, Leiden/Boston: Martinus Nijhoff Publishers.

Burger@Overheid.nl (2006) *Werkschrift BurgerServiceCode*, version 2.2 www.burger.overheid.nl/files/bsc_schrift_versie_2.2._december_2006_.pdf, consulted on 22 November 2010.

Burger@Overheid.nl (2007) *Het geweten van de elektronische overheid. Vijf jaar Burger@Overheid.nl (2002-2007)*, The Hague.

Buruma, Y. (2011) 'Het recht op vergetelheid. Politiële en justitiële gegevens in een digitale

wereld' in D. Broeders, C. Cuijpers & J.E.J. Prins, *De staat van informatie*, WRR verkenning nr. 25, Amsterdam: Amsterdam University Press.

Canhoto, A. & J. Backhouse (2008) 'General Description of the Process of Behavioral Profiling', pp. 47-64 in M. Hildebrandt & S. Gutwirth (eds.) *Profiling the European Citizen. Cross-Disciplinary Perspectives,* Belgium: Springer.

CapGemini Consulting & Ernst & Young (2004) *De koers van de keten. Een verkennend onderzoek naar de consequenties van digitalisering in de bestemmingsplanketen*, Onderzoek in opdracht van de Provincie Noord-Brabant en het Ministerie van VROM, Utrecht.

CapGemini Consulting (2010a) *eRijbewijs. CapGemini onderzoek naar het eRijbewijs en haar relatie met andere initiatieven*, Utrecht.

CapGemini Consulting (2010b) *Interoperabiliteit binnen en tussen sectoren,* Verkenning voor het Forum Standaardisatie naar e-dossiers, verwijsindexen en registers, The Hague.

Caplan, J. & J. Torpey (2001) 'Introduction', pp. 1-12 in J. Caplan & J. Torpey (eds.) *Documenting Individual Identity. The Development of State Practices in the Modern World,* Princeton: Princeton University Press.

Castells, M. (1996, second edition 2000) *The Rise of the Network society, The Information Age: Economy, Society and Culture I*, Cambridge MA: Blackwell.

Centraal Bureau voor Statistiek (2009a) *De digitale economie*, The Hague.

Centraal Bureau voor de Statistiek (2009b) *Integrale Veiligheidsmonitor 2008*, www.cbs.nl/NR/rdonlyres/DD316B79-27F4-4370-A0D4-BE0514248B4B/0/2008integraleveiligheidsmonitorlandelijk.pdf.

Centraal Informatiepunt Onderzoek Telecommunicatie (2010a) *Jaarverslag 2009*, The Hague.

Centraal Informatiepunt Onderzoek Telecommunicatie (2010b) *Eindrapport Audit CIOT en omgevingen 2009*, The Hague 19 April 2010.

Centraal Planbureau (2004) *Zelfevaluatie door het College bescherming persoonsgegevens (CBP) van het toezicht op de verwerking van persoonsgegevens*, The Hague, 30 maart 2004.

Chandler, D. (1996) 'Engagement with Media: Shaping and Being Shaped', *Computer-Mediated Communication Magazine.*

Chavannes, M. (2009) *Niemand regeert. De privatisering van de Nederlandse politiek*, Rotterdam: NRC Boeken.

Choenni, S., E. Leertouwer & T. Busker (2011) 'Klachten over toepassingen van informatietechnologie: analyse van een aantal overheidsbestanden' in D. Broeders, C. Cuijpers & J.E.J. Prins *De staat van informatie*, WRR verkenning nr. 25, Amsterdam: Amsterdam University Press.

Clarke, R. (1988) 'Information Technology and Dataveillance', *Communications of the ACM* 31, 5: 498-512.

Clarke, R. (1994) 'The Digital Persona and Its Application to Data Surveillance', *The Information Society,* 10,2, www.rogerclarke.com/DV/DigPersona.html, consulted on 23 August 2010.

College Bescherming Persoonsgegevens (2006) *Notitie Fraudebestrijding door bestandskoppeling*, The Hague, September 2006.
College Bescherming Persoonsgegevens (2007) Advies Wetsvoorstel implementatie bewaarplicht, 22 January 2007.
College Bescherming Persoonsgegevens (2008) *Jaarverslag 2007,* The Hague.
College Bescherming Persoonsgegevens (2009) *Jaarverslag 2008*, The Hague.
College Bescherming Persoonsgegevens (2010a) *Onderzoek naar de verwerking van het burgerservicenummer en kopie identiteitsbewijs voor de Rijkspas door de minister van Verkeer en Waterstaat*, z2010-00050, 27 May 2010. See www.cbpweb.nl/Pages/med_20100607_rijkspas.aspx.
College Bescherming Persoonsgegevens (2010b) *Rapport over bestandskoppelingen door de SIOD voor de ontwikkeling van risicoprofielen*, The Hague, May 2010.
College Bescherming Persoonsgegevens (2010c) *Jaarverslag 2009*, The Hague.
College en Forum Standaardisatie (2009) *Jaarverslag 2009*, The Hague, 23 February 2010.
Commissie-Brouwer-Korf (2009) *Gewoon Doen. Beschermen van veiligheid en persoonlijke levenssfeer*, Rapport aan de ministers van Justitie en Binnenlandse Zaken, The Hague.
Commissie-Jorritsma (2005) *Publieke dienstverlening, professionele gemeenten. Visie 2015*, The Hague: VNG.
Commissie-Mevis (2001) *Rapport van de Commissie Strafvordelijke gegevensvergaring in de informatiemaatschappij*. Kamerstukken II, 2001/02, 28366, nr. 1.
Commissie-Postma-Wallage (2007) *Het uur van de waarheid*, The Hague.
Commissie-Suyver (2009) *Naar een integrale evaluatie van antiterrorismemaatregelen*, Rapport van de Commissie evaluatie antiterrorismebeleid, The Hague.
Cuijpers, C.M.K.C. & E.J. Koops (2009) 'Begluren en besturen door slimme energiemeters: een ongerechtvaardigde inbreuk op onze privacy', *Privacy en Informatie* 1: 2-8.
Cukier, K. (2010) *Metadata Matters. META: The Rise and Governance of Information about Information. A Report of the 2010 Global Leaders of Information Policy Conference*, Singapore.
Custers, B. (2004) *The Power of Knowledge. Ethical, Legal, and Technological Aspects of Data Mining and Group Profiling in Epidemiology*, Nijmegen: Wolf Legal Publishers.
Deleuze, G. (2002) 'Postscript on Control Societies', pp. 316-321 in T. Levin, U. Frohne & P. Weibel (eds.) *CTRL [SPACE]. Rhetorics of Surveillance from Bentham to Big Brother*, Cambridge, MA: MIT Press.
Deursen, A.J.A.M. van, J.A.G.M. van Dijk & D. Boland (2007) *Elektronische publieke dienstverlening in de toekomst. Opinies over de strategische doelstellingen en perspectieven achter elektronische overheidsdienstverlening*, Research report University of Twente.
Deursen, A.J.A.M. van & J.A.G.M. van Dijk (2010) *Trendrapport Computer- en Internetgebruik 2010. Een Nederlands en Europees perspectief*, Enschede: University of Twente.

Dijk, van J. (2007) 'De e-surfende burger: is de digitale kloof gedicht?', pp. 31-50 in J. Steyaert & J. de Haan (ed.) *Jaarboek ICT en samenleving. Gewoon digitaal,* Amsterdam: Boom.

Dijstelbloem, H. & A. Meijer (2009) *De Migratiemachine. De rol van technologie in het Migratiebeleid*, Amsterdam: Van Gennep.

Dijstelbloem, H. & J.W. Holtslag (2010) 'De veranderende architectuur van het bestuur', pp. 15-54 in H. Dijstelbloem, P. den Hoed, J.W. Holtslag & S. Schouten (eds.) *Het gezicht van de publieke zaak. Openbaar bestuur onder ogen*, WRR-verkenning nr. 23, Amsterdam: Amsterdam University Press.

Donk, W. van de, & P. Depla (1993) 'Wie stuurt de vernieuwing? Raadsinformatiesystemen als ontmoeting van politiek en technologie', *Bestuurskund*e 2, 6.

Donk, W.B.H.J. van de, & O. Meyer (1994) 'Beleid voor informatisering', pp. 29-68 in A. Zuurmond et al. *Informatisering in het openbaar bestuur. Technologie en sturing bestuurskundig beschouwd,* The Hague: VUGA.

Donk, W.B.H.J. van de & P.H.A. Frissen (1994) 'Informatisering, Wetgeving en Sturing', pp. 35-64 in Ph. Eijlander et al. (ed.) *Wetgeven en de maat van de tijd*, Zwolle: Tjeenk Willink.

Donk, W.B.H.J. van de (1997) *De arena in schema. Een verkenning van de betekenis van informatisering voor beleid en politiek inzake de verdeling van middelen onder verzorgingshuizen*, dissertation, Tilburg.

Donk, W.B.H.J. van de & R. van Dael (2005) 'Overheid en ICT: Kroniek van een beleid', pp. 161-196 in M. Lips et al. (ed.) *ICT en openbaar bestuur. Implicaties en uitdagingen van technologische toepassingen voor de overheid*, Utrecht: Lemma.

Ducastel, N. (2008) 'Europese interoperabiliteit: langzaam en zeker?!', pp. 283-293 in S. Zwienink & P. Wisse. (eds.) *Eerlijk zullen we alles delen. Verkenningen naar inter-operabiliteit*, GBO. The Hague: Overheid/Bureau Forum Standaardisatie.

Duivenboden, H.P.M. van (1999) *Koppeling in uitvoering. Een verkennende studie naar de betekenis van het koppelen van persoonsgegevens door uitvoerende overheidsorganisaties voor de positie van de burger als cliënt van de overheid*, Delft: Eburon.

Duivenboden, H.P.M. van et al. (ed.) (2000) *Ketenmanagement in de publieke sector*, Utrecht: Lemma.

Duivenboden, H.P.M. van & M. Rietdijk (2005) *Puzzelen met Prioriteit. Een strategische verkenning van het absorptievermogen van gemeenten met betrekking tot de implementatie van ICT-vernieuwingen.* Onderzoek in opdracht van ministerie van BZK en het VNG, CapGemini: Utrecht.

Dunleavy, P., H. Margetts, S. Bastow & J. Tinker (2006) *Digital Era Governance: IT Corporations, the State, and eGovernment*, Oxford: Oxford University Press.

Dutton, W.H. (1999) *Society on the Line. Information Politics in the Digital A*ge, Oxford: Oxford University Press.

Dworkin, R. (1977) *Taking Rights Seriously*, Cambridge, MA: Harvard University Press.

eCall Driving Group (2005) *eCall Driving Group: Participants*, www.esafetysupport.org/en/ecall_toolbox/index.html, consulted on 3 November 2010.

Edge, D. (1995) 'The Social Shaping of Technology', pp. 14-32 in N. Heap, R. Thomas, G. Einon, R. Mason & H. Mackay (eds.) *Information, Technology and Society,* London: Sage.

EDPS (2006) *Opinion of the European Data Protection Supervisor*, Brussels, 20 January 2006.

Edwards, G. & C.O. Meyer (2008) 'Introduction: Charting a Contested Transformation' in JCMS 46, 1: 1-26.

Eenmalige Adviescommissie ICT en Overheid (2001) *Burger en overheid in de informatiesamenleving. De Noodzaak van institutionele innovatie*, The Hague.

Eerste Kamer (2006-2007) *Behandeling wetsvoorstel BSN*, Kamerstukken I, 30312, B.

Eerste Kamer (2007-2008) *Brief Vaste Commissie voor Binnenlandse Zaken over de notitie burgerservicenummer*, Kamerstukken I, 30312, J.

Eerste Kamer (2008-2009a) *Behandeling wetsvoorstel slimme energiemeters*, Handelingen I, nr. 26.

Eerste Kamer (2008-2009b) *Behandeling herinrichten reisdocumentenadministratie*, Handelingen I, nr. 34: 1563 ff.

Eerste Kamer (2009-2010a) *Verslag Schriftelijk Overleg inzake evaluatie WBP,* Kamerstukken I, 31051, A.

Eerste Kamer (2009-2010b) *Verslag van een rondetafel over het EPD*, Kamerstukken I, 31466, K.

Eerste Kamer (2009-2010c) *Memorie van antwoord – Wijzinging van de Wet gebruik burgerservicenummer in de zorg*, Kamerstukken I, 31466, C.

Eerste Kamer (2009-2010d) *Voorlopig verslag van overleg over Wijziging van de Wegenverkeerswet 1994*, Kamerstukken I, 31896, B.

Eerste Kamer (2009-2010e) *Memorie van Antwoord – Wijziging van de Wegenverkeerswet 1994*, Kamerstukken I, 31896, C.

Eerste Kamer (2009-2010f) *Brief staatssecretaris betreffende de toekenning, het beheer en het gebruik van het Burgerservicenummer*, Kamerstukken I, 30312, L.

Eerste Kamer (2010-2011) *Korte aantekeningen vergadering van de vaste commissies van BZK, de JBZ-Raad, Justitie, OC&W en VWS*, 7 December 2010, www.eerstekamer.nl/behandeling/20101207/korte_aantekening_9/f=/vikzc6ylr2ho.pdf, consulted on 4 January 2011.

Eeten, M. van (2010) *Techniek van de onmacht: Fatalisme in politiek en technologie*, oration Delft.

Eeten, M. van (2011) 'Gedijen bij onveiligheid: afwegingen rond de risico's van informatietechnologie' in D. Broeders, C. Cuijpers & J.E.J. Prins *De staat van informatie*, WRR verkenning nr.25, Amsterdam: Amsterdam University Press.

Eijkman, Q. (2010) 'Liever geen bekende Nederlander zijn. Het mobiliseren van mensenrechten en de bescherming van digitale persoonsgegevens', pp. 65-72 in *16 miljoen BN'ers? Bescherming van persoonsgegevens in het Digitale Tijdperk 47*, Leiden: Stichting NJCM-Boekerij.

Ellul, J. (1954) *La technique ou l'enjeu du siecle*, Paris: Armand Collin.

Ellul, J. (1977) *La systeme technicien*, Paris: Calmann-Levy.

Est, R. van, C. van 't Hof, D. van Harten (ed.) (2007) *RFID: meer keuze, gemak en controle in de digitale publieke ruimte,* The Hague: Rathenau Institute.

European Commission (1999) *Europe: Een informatiemaatschappij voor iedereen*, COM (1999) 687 def.

European Commission (2001) *European Governance, a White Paper*, Brussels, http://eur-ex.europa.eu/LexUriServ/site/en/com/2001/com2001_0428en01.pdf, consulted on 16 November 2009.

European Commission (2002) *Actieplan eEurope 2005: Een informatiemaatschappij voor iedereen,* COM (2002) 263 def.

European Commission (2003) *Ontwikkeling van het Schengeninformatiesysteem II en mogelijke synergie met een toekomstig visuminformatiesysteem (VIS)*, COM (2003) 771 def.

European Commission (2005) *A Fine Balance: Privacy Enhancing Technologies: How to Create a Trusted Information Society – Summary of Conference*, Brussels.

European Commission (2010a) *Communication Overview of Information Mangement in the Area of Freedom, Securityh and Justice*, COM (2010) 385 final.

European Commission (2010b) *Mededeling inzake doorgifte van passagiersgegevens (PNR)*, COM (2010) 492 def.

European Commission (2010c) *Europese Commissie presenteert strategie voor versterking gegevensbeschermingsregels EU*, IP/10/1462.

Expertcommissie informatievoorziening en elektronische dienstverlening SUWI (2005) *De Burger Bediend*, The Hague.

Facebook (2010) Perskamer, www.facebook.com/press/info.php?statistics, consulted on 27 September 2010.

Februari, M. (2008) '*Variaties op de standaard*', The Hague: Forum Standaardisatie *2008*: 91-92.

Ferwerda, H., E. van der Torre & V. van Bolhuis (2010) *Nodale praktijken. Empirisch onderzoek naar het nodale politieconcept, Politie en Wetenschap*, Bureau Beke, COT Institute voor Veiligheid en Crisismanagement, Apeldoorn, Arnhem, The Hague.

Fijnaut, C. (2007) 'De ontwikkeling van de politiële samenwerking in de Europese Unie: verworvenheden en uitdagingen', pp. 109-138 in J. Meeusen & G. Straetmans (eds.) *Politiële en justitiële strafrechtelijke samenwerking in de Europese Unie. Welk evenwicht tussen vrijheid, veiligheid en rechtvaardigheid?*, Antwerp: Intersentia.

Fleck, J. (1993) 'Configurations: Crystallizing Contingency', *International Journal on Human Factors in Manufacturing* 3: 15-36.

Floridi, L. (2005) 'The Ontological Interpretation of Information Privacy', *Ethics and Information Technology:* 185-200.

Florini, A. (1998) 'The End of Secrecy', *Foreign Policy:* 50-63.

Forum Standaardisatie (2010) *Sturen op Open Standaarden. Een handreiking voor overheidsorganisaties*, The Hague.

Foucault, M. (1977) *Discipline and Punish. The Birth of the Prison*, New York: Vintage.

Fountain, J. (2001) 'Paradoxes of Public Sector Customer Service', *Governance: An International Journal of Policy and Administration* 14, 1: 55-73.

Franken, H. (1993) 'Kanttekeningen bij het automatiseren van beschikkingen' in *Beschikken en Automatiseren. Preadvies voor de Vereniging voor Bestuursrecht*, VAR-reeks nr. 110, The Hague.

Fredman, S. (2008) *Human Rights Transformed: Positive Rights and Positive Duties*, Oxford: Oxford University Press.

Frissen, P.H.A. (2009) *Gevaar verplicht. Over de noodzaak van aristocratische politiek*, Amsterdam: Van Gennep.

Frissen, P.H.A. (1989) *Bureaucratische cultuur en informatisering. Een studie naar de betekenis van informatisering voor de cultuur van een overheidsorganisatie*, The Hague: Sdu Uitgeverij.

Frissen, P.H.A. (1996) *De virtuele staat. Politiek, bestuur, technologie: een postmodern verhaal*, Schoonhoven: Academic Service.

Frissen, V. (2004) *De Domesticatie van de Digitale Wereld*, Speech given on acceptance of the professorship of an endowed chair in ICT and Social Change sponsored by the TNO LIFT Fund in the Faculty of Philosophy at Erasmus University Rotterdam. www.publiek-politiek.nl/Bestanden/the-XPIN-files/De-domesticatie-van-de-digitale-wereld-Valerie-Frissen, consulted on 23 August 2010.

Frissen, V.M. (2008) 'Digitaal knutselen. De doorbraak van het wilde denken', pp. 15-27 in V.M. Frissen & J. de Mul (ed.) *De draagbare lichtheid van het bestaan*, Kampen: Klement/Pelckmans.

Fuglsang, L. (2001) 'Three Perspectives in STS in the Policy Context', pp. 35-50 in S. Cutcliffe & C. Mitcham (eds.) *Visions of STS. Cointerpoints in Science, Technology, and Society Studies,* New York: State University of New York Press.

Fung, A., M. Graham & D. Weil (2007) *Full Disclosure: the Perils and Promise of Transparency*, Cambridge: Cambridge University Press.

Garland, D. (2001) *The Culture of Control*, Oxford: Oxford University Press.

Gateway NUP (2009) *Wederzijdse gijzeling in machteloosheid, of de As van het Goede?,* Report NUP-review.

George, A. & A. Bennet (2004) *Case studies and theory development in the social sciences*, Cambridge, MA: MIT Press.

Gilder, G. (1994) *Life after Television: The Coming Transformation of Media and American Life*, New York: W.W. Norton.

Gilliom, J. (2001) *Overseers of the Poor. Surveillance, Resistance, and the Limits of Privacy,* Chicago: University of Chicago Press.

Gómez-Arostegui, H.T. (2005) 'Defining Private Life under the European Convention on Human Rights by Referring to Reasonable Expectations', *California Western International Law Journal* 35: 153-202.

Gomez-Barrosso, J.L., C. Feijoo & E. Karnitis (2008) 'The European Policy for the Development of an Information Society: The Right Path?', *Journal of Common Market Studies* 46 (4): 787-825.

Govcert.nl (2009) *Trendrapport 2009. Inzicht in cybercrime: trends en cijfers*, The Hague: Ministerie van BZK.

Govcert.nl (2010) *Jaarverslag 2009*, The Hague.

Gribnau, J.L.M. (2010) 'Kenbare fouten en navordering. Grondslagen in het licht van automatisering en mensen', *Weekblad Fiscaal Recht*, 2010/214.

Griffioen, H. (2011) *'Location Based Privacy' in Constellaties van publiek-private verantwoordelijkheid*, WRR webpublication, Amsterdam: Amsterdam University Press.

Grijpink, J.H.A.M. (2006a) *Keteninformatisering in kort bestek: theorie en praktijk van grootschalige informatie-uitwisseling*, The Hague: Lemma.

Grijpink, J.H.A.M. (2006b) 'Identiteitsfraude en overheid', *Justitiële Verkenningen* 32, 7: 36-56.

Groot, H. de (2010) *Evidence-Based Public Management*, oration University of Twente, 3 June 2010.

Groothuis, M.M. (2010) 'De Awb en digitalisering', pp. 343-358 in T. Barkhuysen et al. (ed.) *Bestuursrecht harmoniseren: 15 jaar Awb*, The Hague: Boom Juridische Uitgevers.

Guild, E. (2009) *Security and Migration in the 21st Century*, Cambridge: Polity Press.

Gunsteren, H. van (2004) *Gevaarlijk Veilig. Terreurbestrijding in de democratie*, Amsterdam: Van Gennep.

Gunsteren, H. van (2006) *Vertrouwen in de democratie. Over principes van zelforganisatie*, Amsterdam: Van Gennep.

Gunsteren, H. van (2009) 'Burgerschap in Nederland 1992-2008: voortschrijdend inzicht?', *B en M* 36, 1: 41-49.

Haan, J. de (2004) 'ICT en samenleving', pp. 223-264 in *In het zicht van de toekomst, sociaal en cultureel rapport 2004*, The Hague: Sociaal en Cultureel Planbureau.

Haan, J. de & L. van der Laan (2005) *Jaarboek ICT en samenleving. Kennis in netwerken*, Amsterdam: Boom.

Haggerty, K. & R. Ericson (2000) 'The surveillant Assemblage', *British Journal of Sociology* 51, 4: 605-622.

Hampshire, J. & D. Broeders (2010) *The digitalization of European Borders and Migration Controls*, Pilot Study for the Migration to Europe in the Digital Age (MEDIA) project, www.mediaresearchproject.eu/reports/Report2_Borders.pdf, consulted on 11 November 2010.

Haratsch, A. (2006) 'Allgemeine Handlungsfreiheit', pp. 558-572 in F.S.M. Heselhaus & C. Nowak (Hrsg.) *Handbuch der Europäischen Grundrechte*, Munich: Beck.

Harcourt, B.E. (2007) *Against Prediction: Profiling, Policing, and Punishing in an Actuarial Age*, Chicago: University of Chicago Press.

Hayes, B. (2009) *NeoConOpticon. The EU Security-Industrial Complex*. Amsterdam/London: Transnational Institute/Statewatch.

HEC (2007) *Naar een goed gebruik van het burgerservicenummer (BSN)*, Papernote nr. 21, P. Heemskerk et al., The Hague.

Hermans, K. (2010) 'Het gebruik van vingerafdrukken voor opsporingsdoeleinden onder de nieuwe paspoortwet en artikel 8 EVRM', *Nederlands Tijdschrift voor de Mensenrechten/NJCM Bulletin* 1: 35-40.

Hert, P. de & B. de Schutter (2008) 'International Transfers of Data in the Field of JHA: The

Lessons of Europol, PNR and SWIFT', pp. 299-335 in B. Martenczuk & S. van Thiel (eds.) *Justice, Liberty, Security: New Challenges for EU External Relations*. Brussels: VUB Press.

Hert, P. de (2009) *In het licht van de technologie. Pleidooi voor continuïteit en verandering bij gegevensbescherming*, The Hague: College Bescherming Persoonsgegevens.

Hert, P. de (2011) 'Systeemverantwoordelijkheid voor de informatiemaatschappij als positieve mensenrechten verplichting', in D. Broeders, C. Cuijpers & J.E.J. Prins (eds), *De staat van informatie*, WRR verkenning nr.25, Amsterdam: Amsterdam University Press.

Hildebrandt, M. & S. Gutwirth (eds.) (2008) *Profiling the European Citizen. Cross-Disciplinary Perspectives,* Belgium/Netherlands: Springer.

Hildebrandt, M. (2008) 'Defining Profiling: A New Type of Knowledge', pp. 17-45 in M. Hildebrandt & S. Gutwirth (eds.) *Profiling the European Citizen. Cross-Disciplinary Perspectives,* Belgium/Netherlands: Springer.

Hirsch Ballin, E.M.H. (1986) 'De legitimiteit van de selectie van informatie', *Ars Aequi* 35, 11: 726-730.

Hirsch Ballin, E.M.H. (1992) 'Democratie en informatiesamenleving', pp. 77-85 in P.H.A. Frissen et al. (ed.) *Orwell of Athene. Democratie en informatiesamenleving*, The Hague: Sdu.

Hirsch Ballin, E.M.H. (1993) 'De gekoppelde staat', pp. 61-74 in L.A. Geelhoed et al. (ed.) *Wetgeving in Beweging,* Zwolle: Tjeenk Willink.

Hobbing, P. & R. Koslowski (2009) *The Tools Called to Support the 'Delivery' of Freedom, Security and Justice: A Comparison of Border Security System in the EU and in the US*, Ad Hoc Briefing Paper, European Parliament, Directorate-General Internal Policies, Policy Department C, Citizens' Rights and Constitutional Affairs, Committee on Civil Liberties, Justice and Home Affairs, PE 410.681.

Hof, S. van der, R. Leenes & S. Fennell (2009) *Framing Citizen's Identities. The Construction of Personal Identities in New Modes of Government in the Netherland*s, Tilburg.

Hof, S. van der & E. Keymolen (2010) 'Shaping Minors with Major Shifts: Electronic Child Records in the Netherlands', *Information Polity,* 15: 309-322

Hof, C. van 't, R. van Est & F. Daemen (2010) *Check in/Check out. De digitalisering van de openbare ruimte.* The Hague: Rathenau Institute.

Holla, Poelman & Van Leeuwen advocaten (2008), *Brief* 28 maart 2008.

Hoogwout, M. (2010) *De rationaliteit van de klantgerichte overheid. Een onderzoek naar de spanningen die de invoering van het klantdenken bij gemeenten veroorzaakt en de manier waarop gemeenten daarmee omgaan*, Nieuwegein: Uitgeverij Réunion.

Horrocks, I. (2009) ''Experts' and eGovernment. Power, Influence and the Capture of a Policy Domain in the UK', *Information, Communication en Society* 12, 1: 110-127.

Horsley, J. (2007) 'Towards a More Open China?', pp. 54-91 in A. Florini (ed.) *The Right To Know*, Chichester: Columbia University Press.

House of Commons Home Affairs Committee (2008) *A Surveillance Society?*, Fifth Report of Session 2007-08 (2 Volumes), London: Stationery Office.

House of Lords (2007) Schengen Information System (II) (SIS II), Report with Evidence,

9th Report of Session 2006-7 of the House of Lords' European Union Committee, London: The Stationary Office Limited.
House of Lords (2009) Surveillance: Citizens and the State, London: 6 February 2009.
Hout, E. van (2005) 'Kosten en baten van ICT en informatievoorziening in het openbaar bestuur', pp. 257-276 in M. Lips et al. (ed.) *ICT en openbaar bestuur. Implicaties en uitdagingen van technologische toepassingen voor de overheid*, Utrecht: Lemma.
Hoven, J. van den (1998) 'Moral Responsibility, Public Office and Information Technology', pp. 97-106 in I. Snellen & W. van de Donk (eds.) *Public Administration in an Information Age. A Handbook*, Amsterdam: IOS Press.
Hughes, T. (1994) 'Technological Momentum', pp. 101-115 in M. Smith & L. Marx (eds.) *Does Technology Drive History? The Dilemma of Technological Determinism,* Cambridge, MA: MIT Press.
Hurenkamp, M. & M. Kremer (ed.) (2005) *Vrijheid Verplicht. Over tevredenheid en de grenzen van keuzevrijheid*, Amsterdam: Van Gennip.
Huydecoper, S., G. Lekkerkerker & P. van Schelven (2001) 'Van eOverheid en wijze mannen', pp. 57-72 in P. van Schelven et al. (ed.) *E-Government. Virtuele fictie of blijvend toekomstbeeld?,* Nederlandse Vereniging voor Informatietechnologie en Recht, preadviezen *2001,* The Hague: Elsevier.
Hyves (2010) www.hyves.nl, consulted on 16 June 2010.
Infodrome (2001) *Controle geven of nemen. Een politieke agenda voor de informatiesamenleving*, Amsterdam: Otto Cramwinckel.
Informatie Beheer Groep (2009) *Jaarverslag 2008*, Groningen.
Information Commissioner's Office (2007) *Data Protection Strategy Consultation*, Draft.
Johnson, D. G. & J. M. Wetmore (eds.) (2009) *Technology and Society. Building our Sociotechnical Future*, Cambridge, MA: MIT Press.
Johnston, L. & C. Shearing (2003) *Governing Security. Explorations in Policing and Justice*, London: Routledge
Jurgens, E. (2005) 'NJCM: ontdek het parlement! Een aansporing aan het NJCM om het parlement te helpen bij zijn kritiek op verdragen en EU-besluiten in voorbereiding', *Terrorismebestrijding met mensenrechten*, Leiden: NJCM-Boekerij nr. 42.
Kaplan, D. (2009) *Readings in the Philosophy of Technology,* 2nd ed., Lanham, MD: Rowman & Littlefield.
Kearns, I. (2004) *Public Value and eGovernment*, London: Institute for Public Policy Research (IPPR).
Keizer, A.G. (2011) 'De digitale patiënt centraal. Medische informatie in een digitale wereld', in D. Broeders, C. Cuijpers & J.E.J. Prins, *De staat van informatie*, WRR verkenning nr.25, Amsterdam: Amsterdam University Press.
Keymolen, E. (2007) *Onzichtbare zichtbaarheid. Plessner ontmoet profiling* (paper EUR).
Keymolen, E.L.O. & D. Broeders (2010) 'Verloren onschuld. Inzicht en toezicht binnen de Verwijsindex Risicojongeren', pp. 73-89 in W. Pieters et al. (ed.) *Inzicht en toezicht. Controle in de Kennissamenleving*, Jaarboek Kennissamenleving 2010, Amsterdam: Aksant.
Keymolen, E., J.E.J. Prins & C. Raab (2011) 'Trust and ICT: New Challenges for Public

Administration' in I.Th.M. Snellen, M. Thaens & W.B.J.M. van de Donk (eds.) *Public Administration in an Information Age*, IOS Press 2011, forthcoming.

Keymolen, E.L.O. & J.E.J. Prins (2011) 'Jeugdzorg via systemen. De verwijsindex risicojongeren als spin in een digitaal vangnet', in D. Broeders, C. Cuijpers & J.E.J. Prins, *De staat van informatie*, WRR verkenning nr.25, Amsterdam: Amsterdam University Press.

Kielman, H. (2010) *Politiële gegevensverwerking en privacy*, dissertation, Leiden.

Kinkhorst, O. (2000) 'Het RINIS-concept: keteninformatisering in de sociale zekerheid', pp. 175-184 in H. van Duivenboden et al. (ed.) *Ketenmanagement in de publieke sector,* Utrecht: Lemma.

Klein, E. (2003) 'Why Should a Computer Be anything Like a Human Being?'*, I3 Magazine*: 30-32. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.102.8768enrep=rep1entype=pdf, consulted on 17 August 2010.

Knaap, P. van der (2010) 'Veiligheidsbeleid: onderbouwd en effectief? De meerwaarde van beleidstheorieën voor beleid en beleidsevaluatie' *Tijdschrift voor veiligheid* 9, 1: 6-21.

Kohnstamm, J. & L. Dubbeld (2007) 'Glazen samenleving in zicht', *Nederlands Juristenblad* 37: 2369-2375.

Kok, W. de, R. Scholtbach & J. van der Vleuten (2001) 'De onzichtbare hand van de overheid. Over de rol van de overheid en de functie van ICT', pp. 281-302 in H. van Duivenboden & M. Lips (ed.) *Klantgericht werken in de publieke sector. Inrichting van de elektronische overheid*, Utrecht: Lemma.

Koops, B.J. (2006) *Tendensen in opsporing en technologie: Over twee honden en een kalf*, oration, Tilburg.

Koslowski, R. (2008) 'Global Mobility and the Quest for an International Migration Regime', pp. 103-143 in J. Chamie & L. Dall'Oglio (eds.) *International Migration and Development: Continuing the Dialogue: Legal and Policy Perspectives*, Geneva: International Organization for Migration.

Kroes, N. (2010) Memo 10/33, date 09/02/2010, see www.europa.eu/rapid/search Action.do.

Kroon, N. & V. Bekkers (1994) 'Informatiesystemen in Europa: een slagader of een slagveld', pp. 69-82 in A. Zuurmond et al. (ed.) *Informatisering in het openbaar bestuur. Technologie en sturing bestuurskundig beschouwd,* The Hague: VUGA.

Kumar, K. (2004) 'Bringing it All Back Home. A Comment on Iris Young', pp. 187-193 in B. Rössler (ed.) *Privacies. Philosophical Evaluations*, Stanford: Stanford University Press.

Laan, L. van der & J. de Haan (2005) 'ICT in de kennis –en netwerkeconomie', pp. 13-32 in J. de Haan et al. (ed.) *Jaarboek ICT en samenleving. Kennis in netwerken*, Amsterdam: Boom.

Lahav, G. & V. Guiraudon (2000) 'Comparative Perspectives on Border Control: Away from the Border and Outside the State', pp. 55-77 in P. Andreas & T. Snyder (eds.) *The Wall around the West. State Borders and ImmigrationCcontrols in North America and Europe,* Lanham, MD: Rowman and Littlefield.

Landelijk Informatiesysteem Schulden (2009) *Protocol 'Landelijk Informatiesysteem Schulden ter voorkoming van problematische schulden'.*

Latour, B. (1992) 'Where are the Missing Masses? The Sociology of a Few Mundane Artifacts', pp. 226-258 in W. Bijker & J. Law (eds.) *Shaping Technology/Building Society*, Cambridge, MA: MIT Press.

Latour, B. (2005) *Reassembling the Social. An Introduction to Actor-Network-Theory,* Oxford: Oxford University Press.

Leadbeater, C. (2008) We-Think: Mass Innovation, not Mass Production, London: Profile.

Leenes, R., B.J. Koops & L. van der Wees (2010) *Onderzoek naar het gebruik van het Burgerservicenummer (BSN) binnen de keten van de elektronische dienstverlening tussen de overheid en bedrijven. Onderzoek in opdracht van het Ministerie van EZ*, The Hague, 16 July 2010.

Lenk, K. & R. Traunmüller (2007) 'Broadening the Concept of Electronic Government', in *Designing eGovernment*, The Hague/Boston: Kluwer Law International 2007.

Leukfeldt, E.R., M.M.L. Domenie & W.Ph. Stol (2010) *Verkenning Cybercrime in Nederland 2009*, Veiligheidsstudies. The Hague: Boom Juridische Uitgevers.

Levin, A. & P. Sánchez Abril (2009) 'Two Notions of Privacy Online', *Vanderbilt Journal of Entertainment and Technology Law* 11, 4: 1001-1051.

Liberatore, A. (2005) *Balancing Security and Democracy: the Politics of Biometric Identification in the European Union*, EUI Working Papers, RSCAS see 2005/30.

Liebenau, J. & J. Backhouse (1990) *Understanding Information: An Introduction*, London: Macmillan.

Lips, M. S. van der Hof, J.E.J. Prins, A.A.P. Schudelaro & M. de Vries (2005) *Issues of Online Personalisation and Commercial and Public Service Delivery*. Nijmegen: Wolf Legal Publishers, 2005.

Lips, A.M.B., J.A. Taylor & J. Organ (2009) 'Service Transformation Towards Citizen-Centric Government? The Evolution of a Smart Card Application in UK Local Government', pp. 66-82 in A.J. Meijer, K. Boersma & P. Wagenaar (eds.) *ICTs, Citizens en Governance: After the Hype*!, Amsterdam: IOS Press Series 'Innovation and the Public Sector'.

Loon, M. van (2010) *Goed opdrachtgeverschap jegens ICTU*, WRR web publication nr.50, www.wrr.nl.

Lor, P. & J. Britz (2007) 'Is a Knowledge Society Possible without Freedom of Access to Information?', *Journal of Information Science* 33, 4: 387-397.

Lubbe, J.C.A. van der (2002) 'Van een informatie- naar een Kennismaatschappij. De rol van techniek', pp. 31-116 in H. Dijstelbloem & C.J. Schuyt (ed.) *De publieke dimensie van kennis*, The Hague: Sdu uitgevers.

Luhmann, N. (1979) *Trust and Power*, H. Davis (transl.), New York: Wiley.

Lyon, D. (1994) *The Electronic Eye. The Rise of Surveillance Society*, Cambridge: Polity Press.

Lyon, D. (2003) *Surveillance after September 11*. Cambridge: Polity Press.

Lyon, D. (2007) *Surveillance Studies. An Overview*, Cambridge: Polity Press.

Lyon, D. (2009) *Identifying Citizens. ID Cards as Surveillance*, Cambridge: Polity Press.

MacGillavry, E.C. (2000) *Meewerken aan strafvordering door banken en Internet Service Providers. Een onderzoek naar wetgeving en praktijk*, Gouda: Quint.

MacKenzie, D.A. & J. Wajcman (eds.) (1985) *The Social Shaping of Technology*, Milton Keynes: Open University Press.

MacKenzie, D.A. (1999a) 'The Certainty trough', pp. 43-46 in W.H. Dutton (ed.) *Society on the Line. Information Politics in the Digital A*ge, Oxford: Oxford University Press.

MacKenzie, D.A. (1999b) 'Technological Determinism', pp. 39-41 in W.H. Dutton (ed.) *Society on the Line. Information Politics in the Digital A*ge, Oxford: Oxford University Press.

Maes, R. (2003) 'Informatiemanagement in kaart gebracht', *PrimaVera Working Paper 2003-02,* Amsterdam: Amsterdam University.

Magnet, S. (2009) 'Using Biometrics to Revisualize the Canada-US border', pp. 359-376 in I. Kerr et al. (eds.) *Lessons from the Identity Trail. Anonymity, Privacy and Identity in a Networked Society*, Oxford: Oxford University Press.

Mansell, R. & R. Silverstone (eds.) (1996) *Communication by Design: The Politics of Information and Communication Technologies*, Oxford: Oxford University Press.

Marx, G. (2001) 'Identity and Anonymity: some Conceptual Distinctions and Issues for Research', pp. 311-327 in J. Caplan & J. Torpey (eds.) *Documenting Individual Identity. The Development of State Practices in the Modern World,* Princeton: Princeton University Press.

Mayer-Schönberger, V. & D. Lazer (2007) 'From Electronic Government to Information Government' in V. Mayer-Schönberger and D. Lazer (eds.) *Governance and Information Technology: from Electronic Government to Information Government,* Massachusetts: MIT Press.

Mayer-Schönberger, V. (2009) *Delete. The Virtue of Forgetting in the Digital Age*, Princeton: Princeton University Press.

Meijer, A. (2004) *Vreemde ogen dwingen. De betekenis van internet voor maatschappelijke controle in de publieke sector*, The Hague: Boom Juridische Uitgevers.

Meijer, A. (2009) 'Informatietechnologie en verantwoordelijkheid: een onbeheersbare migratiemachine', pp. 157-190 in H. Dijstelbloem & A. Meijer (ed.) *De Migratiemachine. De rol van technologie in het Migratiebeleid*, Amsterdam: Van Gennep.

Meijer, A., G.J. Brandsma & S. Grimmelikhuijsen (2010) 'Transparantie als fictieve verantwoording', *Bestuurswetenschappen* 4: 8-27.

Meijer, A. (2011) 'Overheidsverantwoordelijkheid in het informatietijdperk: een pleidooi voor het creëren van genormeerde experimenteerruimte' in D. Broeders, C. Cuijpers & J.E.J. Prins (eds) *De staat van informatie*, WRR verkenning nr.25, Amsterdam: Amsterdam University Press.

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) (1998) *Actieprogramma Elektronische Overheid. Een efficiëntere en effectievere overheid op de elektronische snelweg*, The Hague.

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (2000) *Contract met de Toekomst, een visie op de elektronische relatie overheid-burger*, The Hague.

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (2010) *Staat van het bestuur 2010*, The Hague.
Ministerie van Economische Zaken (1994) *Nationaal Actieprogramma Elektronische Snelwegen*, The Hague.
Ministerie van Economische Zaken e.a. (1999) *Digitale Delta. Nederland online*, The Hague.
Ministerie van Economische Zaken (2008) *ICT Agenda 2008-2011. De gebruiker centraal in de digitale dienstenmaatschappij*, The Hague, June 2008.
Ministerie van Economische Zaken, Landbouw en Inovatie, *Digitale Agenda.nl: ICT voor innovatie en economischge groei*, The Hague 2011.
Ministerie van Justitie (2010) *Visie op biometrie in de identiteitsketen publieke sector*, The Hague, Programma VIPS, July.
Ministerie van Sociale Zaken en Werkgelegenheid (SZW) (2010) *Strategische Kennisagenda editie 2010,* The Hague.
Ministerie van Sociale Zaken en Werkgelegenheid & Ministerie van Volksgezondheid Welzijn en Sport (VWS) (2010) *Programma Stroomlijning Indicatieprocessen in Zorg en Sociale Zekerheid 2006-2009*, The Hague.
Mitrakas, A. (1997) *Open EDI and Law in Europe,* The Hague: Kluwer Law International.
Mitsilegas, V. (2009) 'The Borders Paradox. The Surveillance of Movement in a Union without Internal Frontiers', pp. 33-64 in H. Lindahl (ed.) *A Right to Inclusion and Exclusion? Normative Faultlines of the EU's Area of Freedom, Security and Justice*, Oxford: Hart.
Mom, P. (2010) 'Zesje voor midoffice Logica', *Automatiseringsgids*, 23 April.
Monahan, T. (ed.) (2006) *Surveillance and Security. Technological Politics and Power in Everyday Life,* London: Routledge.
Mul, de J. (2010) 'Keuzedelirium: Over de paradox van de keuzevrijheid', *Database Delirium*, Amsterdam: Bert Bakker.
Mul, J. de (2003) *Cyberspace Odyssee*, Kampen: Klement.
Mul, J. de, E. Müller & A. Nusselder (2001) *ICT de baas? Informatietechnologie en menselijke autonomie,* Onderzoeksprogramma Internet en Openbaar Bestuur, The Hague.
Mulder, K.F. (2006) 'Managing the Dynamics of Technology in Modern Day Society', pp.109-130 in R.M. Verburg et al. (eds.) *Managing Technology and Innovation, an Introduction,* New York: Routledge.
Mulgan, R. (2000) ''Accountability': An Ever-Expanding Concept?', *Public Administration* 78, 3: 555-572.
Müller-Wille, B. (2008) 'The Effect of International Terrorisme on EU Intelligence Co-Operation', *JCMS* 46, 1: 49-74.
Nass, C., J. Steuer & E. Tauber (1994) 'Computers are Social Actors', *Human Factors in Computing Systems*, April: 72-78.
Nass, C., Y., Moon, B. Fogg, B. Reeves & D. Dryer (1995) 'Can Computer Personalities Be Human Personalities?', *Human-Computer Studies* 43: 223-229.
Nationaal uitvoeringsprogramma dienstverlening en eOverheid (2008) *Nationaal Uitvoeringsprogramma Dienstverlening en eOverheid: Burger en bedrijf centraal*, 1 December 2009, see www.e-overheid.nl.

Nationale Ombudsman (2008) Rapport 2008/242, The Hague.
Nationale Ombudsman (2009a*) De burger in de ketens. Verslag van de Nationale Ombudsman over 2008*, The Hague.
Nationale Ombudsman (2009b) Rapport 2009/015, The Hague.
Nationale Ombudsman (2010a) *Toets een 1. . ., toets een 2. . ., toets een 3. . . Wat kan ik voor u doen? Een onderzoek naar de telefonische dienstverlening door de overheid*, Report 2010/010, The Hague.
Nationale Ombudsman (2010b) *Voorbij het conflict. Verslag van de Nationale Ombudsman over 2009*, The Hague.
National Ombudsman (2010c) *Toegang verboden. Onderzoek naar de opname van vreemdelingen in het Schengen Informatie Systeem en de informatievoorziening hierover*, Report 2010/115, The Hague.
Naughton, J. (2010a) 'The Internet: Everything You ever Need to Know', *The Observer*, 20 June 2010.
Naughton, J. (2010b) 'Live with the WikiLeakable World or Shut down the Net. It's Your Choice', *The Guardian*, 6 December 2010.
Neuman, L. & R. Calland (2007) 'Making the Law Work: The Challenges of Implementation' in A. Florini (ed.) *The Right to Know*, Chichester: Columbia University Press.
Noordegraaf, M., A.B. Ringeling & F.J.M. Zwetsloot (ed.) (1995) *De ambtenaar als publiek ondernemer*, Bussum: Countinho.
NRC Next (2010) 'Pats, boem. En geen sporen. Maar de auto vertelt meer', 26 April 2010.
Nussbaum, M.C. (2000) 'The Costs of Tragedy: Some Moral Limits of Cost-Benefit Analysis', *The Journal of Legal Studies* 29, S2: 1005-1036.
Nusselder, A. (2007) 'The Virtual Ego and the Cyborg', *Journal of European Psychoanalysis* 25, 2. www/psychomedia.it/jep/number25/nusselder.htm, consulted on 17 August 2010.
OECD (2008) *OECD Information Technology Outlook 2008*, Paris.
Olsthoorn, P. (2010) *De macht van Google*, Utrecht: Kosmos Uitgevers.
Orwell, G. (1946) *Animal Farm*, San Diego: Harcourt.
Osborne, D. & T. Gaebler (1992) *Reinventing Government: How the Entrepreneurial Spirit is Transforming the Public Sector,* Reading: Addison Wesley.
Oudshoorn, N. & T. Pinch (eds.) (2003) *How Users Matter: The Co-construction of Users and Technology*, Cambridge, MA: MIT Press.
Overkleeft-Verburg, M. (2009) 'Basisregistraties en rechtsbescherming. Over de dualisering van de bestuursrechtelijke rechtsbetrekking', *Nederlands Tijdschrift voor Bestuursrecht* 2009, nr. 4.
Palfrey, J. & U. Gasser (2008) *Born Digital. Understanding the First Generation of Digital Natives*, New York: Basic Books.
Petri, G. (2008) 'Clinger-Cohen Act voorbeeld voor Nederlandse overheid', *Automatisering Gids* 8, The Hague: Sdu Uitgevers.
Pinch, T. J. & W.E. Bijker (1984) 'The Social Construction of Facts and Artefacts: or How the Sociology of Science and Technology Might Benefit Each Other', *Social Studies of Science* 14: 399-441.

Pluut, B. (2010) *Het landelijk EPD als blackbox*, WRR web publication nr. 45, www.wrr.nl.
Porter, M.P. (1995) *Trust in Numbers. The Pursuit of Objectivity in Science and Public Life,* Princeton: Princeton University Press.
Posner, R.A. (1984) 'An Economic Theory of Privacy', pp. 333-345 in F.D. Schoeman (ed.) *Philosophical Dimensions of Privacy: An Anthology*, Cambridge: Cambridge University Press.
Potters, P. & M. de Vreeze (2010) eCall Blackbox. WRR web publication nr. 48, www.wrr.nl.
Power, M. (2005) 'The Theory of the Audit Explosion', pp. 326-344 in E. Ferlie et al. (eds.) *The Oxford Handbook of Public Management*, Oxford: Oxford University Press.
Prins, J.E.J. (2007) 'Technocratie en de toekomstagenda van de Nationale Ombudsman', pp. 111-134 in *Werken aan behoorlijkheid. De Nationale Ombudsman in zijn context (jubileumbundel 25 jaar Nationale Ombudsman)*, The Hague: Boom Juridische Uitgevers.
Prins, J.E.J. (ed.) (2007) *Designing eGovernment*, The Hague: Kluwer Law International.
Prins, J.E.J. (2009) 'Name, Shame and Everlasting Blame', *Nederlands Juristenblad* 84, 3: 119.
Prins, J.E.J. (2010a) 'Burgers en hun privacy: over verhouding en houding tot een ongemakkelijk bezit', pp. 1-14 in J.E.J. Prins (ed.) *16 miljoen BN'ers? Bescherming van persoonsgegevens in het Digitale Tijdperk*, Leiden: Stichting NJCM-Boekerij.
Prins, J.E.J. (2010b) 'Discriminatiesignalen' NJBlog.nl, http://njblog.nl/2010/01/11/discriminatiesignalen/
Raab, C. (2009) 'Identity: Difference and Categorization', pp. 227-244 in I. Kerr, V. Steevens, C. Lucock (eds.) *Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society*, Oxford: Oxford University Press.
Raad van Hoofdcommissarissen (2005) *Politie in ontwikkeling*.
Raad van Hoofdcommissarissen (2009) *Beelden van de Samenleving. Visie op camera-toezicht in een netwerksamenleving*.
Raad van State (2009) *Jaarverslag over 2008*, The Hague.
Raad van State (2010) *Jaarverslag over 2009,* The Hague.
Raad voor Cultuur & Raad voor het Openbaar Bestuur (2008) *Informatie: grondstof met toekomstwaarde. Contouren van een visie op de rol en betekenis van informatie*, The Hague.
Raad voor het Openbaar Bestuur (1998) *Dienen en verdienen met ICT. Over de toekomstige mogelijkheden van de publieke dienstverlening*, The Hague.
Raad voor het Openbaar Bestuur (2010a) *Vertrouwen op democratie,* The Hague.
Raad voor het Openbaar Bestuur (2010b) *Het einde van het blauwdruk-denken. Naar een nieuwe inrichting van het openbaar bestuur*, The Hague.
Rathenau Institute (1998) *Persoonsgegevens in de informatiemaatschappij*. Berichten aan het Parlement, The Hague: Rathenau Institute.
Rathenau Institute, de Consumentenbond en ECP.nl (2007) *RFID bewustzijn van consumenten: Hoe denken Nederlanders over Radio Frequency Identification?*, The Hague.
Rathenau Institute (2008) *Midden in de maatschappij*, Jaarverslag 2007, The Hague.

Rathenau Institute (2010) *Wat is dat eigenlijk, menselijk leven?,* Jaarverslag 2009, The Hague: http://epub02.publitas.nl/36/2/magazine.php#/spreadview/18/, consulted on 11 September 2010.

Reding, V. (2010) *The Challenges Ahead for the European Union*, Keynote Speech at the Data Protection Day 28 January 2010, European Parliament, Brussels.

Reeves, B. & Clifford Nass (1996) *The Media Equation*, Cambridge: Cambridge University Press.

Regeerakkoord (2010) *Vrijheid en Verantwoordelijkheid. Regeerakkoord VVD-CDA*, The Hague.

Rijksarchiefinspectie (2005) *Dementerende Overheid*, The Hague.

Rijksdienst voor het Wegverkeer (2008) *Chip op het rijbewijs,* Verkenning versie 2.1, The Hague.

RINIS (2010) *RINIS Actueel*, June 2010.

Robinson, N. et al. (2010) *Security, at what Cost? Quantifying People's Trade-offs across Liberty, Privacy and Security*, Cambridge: RAND Europe.

Ronfeldt, D. (1992) 'Cyberocracy Is Coming', *Information Society* 8: 243-296.

Rozemond, K. (2010) 'De droom van Beccaria. Over het strafrecht en de nodale veiligheidszorg', *Rechtsfilosofie en Rechtstheorie*, 2: 158-175.

Schenk-Geers, A.C.M. (2007) *Internationale fiscale gegevensuitwisseling en de rechtsbescherming van de belastingplichtige*, dissertation, Tilburg.

Schermer, B.W & T. Wagemans (2009) *Onze digitale schaduw. Een verkennend onderzoek naar het aantal databases waarin de gemiddelde Nederlander geregistreerd staat*, Considerati, for CBP.

Schinkel, W. (2009) 'De nieuwe preventie. Actuariële archiefsystemen en de nieuwe technologie van veiligheid', *Krisis. Tijdschrift voor Actuele Filosofie* 2: 1-21.

Schravendeel, D. & S. Luitjens (2001) 'Een vernieuwde gegevenshuishouding voor de overheid. Doelstelling, inhoud en werkwijze van het programma Stroomlijning Basisgegevens', pp. 347-362 in H. van Duivenboden & M. Lips (ed.) *Klantgericht werken in de publieke sector. Inrichting van de elektronische overheid*, Utrecht: Lemma.

Schreijenberg, A., J. Koffijberg & S. Dekkers (2009) Eindrapport Evaluatie cameratoezicht op openbare plaatsen, Amsterdam: Regioplan.

Schwartz, B. (2004) *The Paradox of Choice. Why More Is Less. How the Culture of Abundance Robs Us of Satisfaction*, New York: Harper Collins.

Scott, J. (1998) *Seeing Like a State. How Certain Schemes to Improve the Human Condition Have Failed,* New Haven: Yale University Press.

Sheptycki, J. (2007) 'Transnational Crime and Transnational Policing', *Sociology Compass* 1, 2: 485-498.

Shrader-Frechette, K. (1992) 'Technology, Bayesian Policymaking, and Democratic Process', pp. 123-137 in L. Winner (ed.) *Democracy in a Technological Society*, Dordrecht: Kluwer.

Silverstone, R. & E. Hirsch (eds.) (1992) *Consuming Technologies: Media and Information in Domestic Spaces*, New York: Routledge.

Simon, H. (1956) 'Rational Choice and the Structure of the Environment', *Psychological Review* 63: 129-138.

Singh, S. (2007) 'Grassroots Initiatives' in A. Florini (ed.) *The Right to Know,* Chichester: Columbia University Press.

Snellen, I. (1992) 'Het Nederlandse parlement in een geïnformatiseerde samenleving', pp. 301-318 in P. Frissen et al. (ed.) *Orwell of Athene. Democratie en informatiesamenleving*, The Hague: Sdu.

Snellen, I. (1994) 'De revolutionaire werking van informatie- en communicatietechnologie in het openbaar bestuur', pp. 417-432 in A. Zuurmond et al. (ed.) *Informatisering in het openbaar bestuur. Technologie en sturing bestuurskundig beschouwd,* The Hague: VUGA.

Snellen, I. (2005) 'eGovernment. A Challenge for Public Management', pp. 398-421 in E. Ferlie et al. (eds.) *The Oxford Handbook of Public Management*, Oxford: Oxford University Press.

Snijder, M. (2010) *Het biometrische paspoort in Nederland*, WRR web publication nr.51, www.wwr.nl.

Snijders, T. (2010) Chief Information Officers bij de Rijksoverheid, in D. Broeders, C. Cuijpers & J.E.J. Prins *De staat van informatie*, WRR verkenning nr.25, Amsterdam: Amsterdam University Press.

Sociaal en Cultureel Planbureau (2004) *In het zicht van de toekomst*, The Hague.

Sociaal en Cultureel Planbureau (2008) *Sociale veiligheid ontsleuteld. Veronderstelde en werkelijke effecten van veiligheidsbeleid*, The Hague.

Socialistische Partij (2008) *ICT bij de overhead, wondermiddel of hoofdpijndossier?,* www.sp.nl/service/rapport/080704_ictbijdeoverheid.pdf.

Solove, D.J. (2004) *The Digital Person*, New York: New York University Press.

Solove, D. (2007) *The Future of Reputation, Gossip, Rumor and Privacy on the Internet*, New Haven, CT: Yale University Press.

Solove, D.J. (2008) *Understanding Privacy*, Cambridge, MA: Harvard University Press.

Staatscommissie Grondwet (2010) *Rapport Staatscommissie Grondwet*, The Hague.

Stevens, B. (2004) 'The Emerging Security Economy: an Introduction' in OECD *The Security Economy*, Paris: OECD.

Stevens, T., J. Elliott, A. Hoikkanen, I. Maghiros & W. Lusoli (2010) *The State of the Electronic Identity Market: Technologies, Infrastructure, Services and Policies*, JRC Scientific and Technical Reports, Luxembourg: Publications Office of the European Union.

Stirling, A. (2008) "Opening up' and 'Closing down", S*cience, Technology and Human Values* 33, 2: 262-294.

Straten, G.F.M. (1996) *In de beslotenheid van het openbaar bestuur. De institutionalisering van informatietechnologie binnen de bevolkingsadministratie*, Utrecht.

Tadros, V. (2006) 'Power and the Value of Privacy', pp. 105-120 in E. Claes et al. (eds.) *Privacy and the Criminal Law*, Antwerp: Intersentia

Taylor, J.R. & E.J. van Every (1993) *The Vulnerable Fortress. Bureaucratic Organization and Management in the Information Age,* Toronto: Toronto University Press.

Teeuw, W.B. & A.H. Vedder (eds.) (2008) *Security Applications for Converging Technologies. Impact on the Constitutional State and Legal Order*, WODC.

Thaens, M. (1998) *De procesbenadering van ICT-evaluatie. De rol van evaluatie in het besluitvormingsproces over investeringen in informatie- en communicatietechnologie binnen een organisatie*, Delft: Eburon.

Tiemeijer W.L. (2006) *Het geheim van de burger: over staat en opinieonderzoek*, Amsterdam: Aksant.

Tiemeijer, W.L. (2009) 'Slotbeschouwing', pp. 293-311 in W.L. Tiemeijer, C.A. Thomas & H.M. Prast (eds.) *De menselijke beslisser: Over de psychologie van keuze en gedrag*, WRR-verkenning nr. 22, Amsterdam: Amsterdam University Press.

TNO (2009) *Marktrapportage elektronische communicatie,* September 2009.

Torpey, J. (1998) 'Coming and Going: on the State Monopolization of the Legitimate Means of Movement', *Sociological Theory* 16, 3: 239-259.

Torpey, J. (2000) *The Invention of the Passport; Surveillance, Citizenship and the State.* Cambridge: Cambridge University Press.

Trouw (2010) 'Australische politie start onderzoek naar Google', www.trouw.nl/nieuws/wereld/article3088346.ece/Australische_politie_start_onderzoek_naar_Google.html, consulted on 18 June 2010.

Tsoukas, H. (1997) 'The Tiranny of Light. The Temptations and the Paradoxes of the Information Society', *Futures* 29, 9: 827-843.

Tweede Kamer (1999-2000) *Motie over bevordering van de ontwikkeling en het gebruik van Privacy Enhancing Technologies*, Kamerstukken II, 25892, nr. 31.

Tweede Kamer (1997-1998) *Nota wetgeving voor de elektronische snelweg*, Kamerstukken II, 25880, nr. 2.

Tweede Kamer (2000-2001a) *Verslag algemeen overleg op 21 juni 2001 over biometrie in reisdocumenten en elektronische identiteitskaart*, Kamerstukken II, 25764, nr. 17.

Tweede Kamer (2000-2001b) *Actieprogramma Elektronische overheid - Nota De elektronische overheid aan het begin van de 21e eeuw*, Kamerstukken II, 26 387, nr. 9.

Tweede Kamer (2000-2001c) *Nota Kaderstellende visie op toezicht*, Kamerstukken II, 27 831, nr. 1.

Tweede Kamer (2004-2005) *Brief inhoudend 'spoorboekje' voor implementatie EPD*, Kamerstukken II, 27529, nr. 15.

Tweede Kamer (2005-2006a) *Memorie van Toelichting Wet algemene bepalingen burgerservicenummer*, Kamerstukken II, 30312, nr. 3.

Tweede Kamer (2005-2006b) *Brief inzake modernisering van de overheid*, Kamerstukken II, 29362, nr. 101.

Tweede Kamer (2005-2006c) *Motie Slob - Wet algemene bepalingen burgerservicenummer*, 30312, nr. 15.

Tweede Kamer (2006-2007) *Brief inhoudend Voortgangsrapportage ICT in de zorg*, Kamerstukken II, 27529, nr. 29.

Tweede Kamer (2007-2008a) *Memorie van Toelichting bij wijziging Paspoortwet*, Kamerstukken II, 31324 (R1844), nr. 3 (Reprint).

Tweede Kamer (2007-2008b) *Brief inzake project Veiligheid begint bij voorkomen*, Kamerstukken II, 28684, nr. 119.

Tweede Kamer (2008-2009a) *Behandeling van het wetsvoorstel Wijziging van wet gebruik*

burgerservicenummer in de zorg, Handelingen II, 31466, nr. 45: 3920-3941.
Tweede Kamer (2008-2009b) *Behandeling van het wetsvoorstel Wijziging van wet gebruik burgerservicenummer in de zorg*, Handelingen II, 31466, nr. 45: 3942-3959.
Tweede Kamer (2008-2009c) *Verslag algemeen overleg van 30-10-2008 over de software van de OV-chipkaart en deurpasjes*, Kamerstukken II, 23645, nr. 274.
Tweede Kamer (2008-2009d) *Brief minister over antiterrorismebeleid*, Kamerstukken II, 29754, nr. 164.
Tweede Kamer (2008-2009e) *Brief minister en staatssecretaris over advies 'Informatie: grondstof met toekomstwaarde'*, Kamerstukken II, 29362, nr. 156.
Tweede Kamer (2008-2009f) *Memorie van Toelichting – Wijziging van onder meer Boek 2 van Burgerlijk Wetboek en de Wet documentatie vennootschappen*, Kamerstukken II, 31948, nr. 3.
Tweede Kamer (2009-2010a) *Brief inzake modernisering GBA*, Kamerstukken II, 27859, nr. 38.
Tweede Kamer (2009-2010b) *Brief staatssecretaris over preventie en bestrijding van stille armoede en sociale uitsluiting*, Kamerstukken II, 24515, nr. 170.
Tweede Kamer (2009-2010c) *Informatiehuishouding van de politie*, Kamerstukken II, 29 628, nr. 217.
Tweede Kamer (2009-2010e) *Wijziging van de Wet houdende wijziging van de Elektriciteitswet 1998 en de gaswet*, Kamerstukken II, 2009/10, 32374, nrs. 1-4.
Tweede Kamer (2009-2010f) *Evaluatie Wet bescherming persoonsgegevens*, Kamerstukken II, 2009/10, 31051, nr. 6.
Tweede Kamer (2009-2010g) *Brief inzake Voortgangsrapportage landelijke infrastructuur voor gegevensuitwisseling in de zorg*, Kamerstukken II, 27529, nr. 61.
Tweede Kamer (2009-2010h) *Wetsvoorstel overige fiscale maatregelen 2010,* Kamerstukken II, 32129, nr. 2.
Tweede Kamer (2009-2010i) *Brief inzake modernisering GBA,* Kamerstukken II, 27859, nr. 30.
Tweede Kamer (2009-2010j) *Kabinetsstandpunt advies Commissie Brouwer-Korf en evaluatie van de Wet bescherming persoonsgegevens*, Kamerstukken II, 31051, nr. 5.
Tweede Kamer (2009-2010k) *Brief inzake Modernisering van de overheid*, Kamerstukken II, 29362, nr. 157.
Tweede Kamer (2010-2011a) *Algemeen Overleg over Nederlandse reisdocumenten*, Kamerstukken II, 25764, nr. 44.
Tweede Kamer (2010-2011b) *Algemeen Overleg met de vaste Commissie voor Financiën*, 31066, nr. 95.
Tweede Kamer (2010-2011c) *Kabinetsreactie Digitale Agenda voor Europa*, Kamerstukken II, 21501-332, nr. 294.
Tweede Kamer (2010-2011e) *Fiche inzake doorgifte van PNR-gegevens,* Kamerstukken II, 22112, nr. 1081.
Tweede Kamer 2010-2011f, *Kentekenherkenning boven de A28*, Bijlage bij Kamerstukken 31051, nr. 8.
Tweede Kamer (2010-2011g) *Kamervragen over het ten onrechte opslaan van kentekengegevens van burgers*, 2010Z19218.

United Nations (2008) *From eGovernment to Connected Governance, United Nations eGovernment Survey 2008*, New York.

United Nations (2010) *Leveraging eGovernment at a time of financial and economic crisis*, *United Nations eGovernment Survey 2010*, New York.

Verbeek, J.P.G.M. (2010) 'Grensoverschrijdende toegang tot politiële databases', pp. 29-34 in L.H.C. Bertram & D.H. van Ekelenburg (eds.) *Opsporingsinformatie vrij verkrijgbaar in Europa?*, Deventer: Kluwer.

Verhey, L.F.M. (1992) *Horizontale werking van grondrechten, in het bijzonder het recht op privacy*, Zwolle: W.E.J. Tjeenk Willink.

Verhoeven, I. (2009) *Burgers tegen beleid. Een analyse van dynamiek in politieke betrokkenheid*, Amsterdam: Aksant.

VNO-NCW (2005) *Brief aan de leden van de Vaste Tweede Kamer Commissies voor Binnenlandse Zaken en Koninkrijksrelaties, Economische Zaken en Justitie*, The Hague, 28 October 2005, www.eerstekamer.nl/behandeling/20080303/brief_van_vno_ncw_aan_de_tweede/f=/w30312ibijl2.pdf.

Vereniging van Nederlandse Gemeenten (2008) *Brief Vereniging van Nederlandse Gemeenten met een reactie op de conceptwetgeving Verwijsindex*, The Hague, Nederlandse Vereniging van Gemeenten, 12 March 2008.

Vereniging van Nederlandse Gemeenten (2010) *Thorbecke 2.0: naar een vernieuwde Nederlandse overheid*, VNG-discussienotitie 23 March 2010, see www.vng.nl.

Volokh, E. (2000) 'Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking about You', *Stanford Law Review* 52: 1049 ff.

Waldron, J. (2007) 'Is This Torture Necessary?', *The New York Review of Books* 54: 16 ff. (25 October 2007).

Warren, S.D. & L.D. Brandeis (1890) 'The right to Privacy', *Harvard Law Review* 4: 193 ff.

Wetenschappelijke Raad voor het Regeringsbeleid (1998) *Staat zonder land. Een verkenning van bestuurlijke gevolgen van informatie- en communicatietechnologie*, Rapporten aan de Regering nr. 54, The Hague: Sdu Uitgevers.

Wetenschappelijke Raad voor het Regeringsbeleid (2002) *Van oude naar nieuwe kennis. De gevolgen van ICT voor het kennisbeleid*, Rapporten aan de regering nr. 61, The Hague: Sdu Uitgevers.

Wetenschappelijke Raad voor het Regeringsbeleid (2008a) *Innovatie vernieuwd: Opening in viervoud*, Rapporten aan de regering nr. 80, Amsterdam: Amsterdam University Press.

Wetenschappelijke Raad voor het Regeringsbeleid (2008b) *Onzekere veiligheid. Verantwoordelijkheden rond fysieke veiligheid*, Rapporten aan de regering nr. 82, Amsterdam: Amsterdam University Press.

Whitson, J. & K.D. Haggerty (2008) 'Identity Theft and the Care of the Virtual Self', *Economy and Society* 37, 4: 571-593.

Williams, R. & D. Edge (1996) 'The Social Shaping of Technology', pp. 53-67 in W.H. Dutton (ed.) *Information and Communication Technologies. Visions and Realities,* Oxford: Oxford University Press.

Williams, R. (1999) 'The Social Shaping of Technology', pp. 41-43 in W.H. Dutton (ed.) *Society on the Line. Information Politics in the Digital A*ge, Oxford: Oxford University Press.

Winter, H.B. et al. (2008) *Wat niet weet, wat niet deert. Een evaluatieonderzoek naar de werking van de Wet bescherming persoonsgegevens in de praktijk*, The Hague: WODC.

Wisse, P. (2008) 'Semantiek, interoperabiliteit en infrastructuur', pp. 382-391 in S. Zwienink & P. Wisse (eds.) *Eerlijk zullen we alles delen*, The Hague: Forum Standaardisatie.

Witteveen, W.J. (2010) 'Kafka en de verbeelding van de bureaucratie', *RegelMaat* 25, 4: 218-226.

Woolgar, S. (1996) 'Technologies as Cultural Artefacts', pp. 88-102 in W.H. Dutton (ed.) *Society on the Line. Information Politics in the Digital A*ge, Oxford: Oxford University Press.

Wyatt, S. (2003) 'Non-Users Also Matter', pp. 67-80 in N. Oudshoorn & T. Pinch (eds.) *How Users Matter: The Co-construction of Users and Technology*, Cambridge, MA: MIT Press.

Zedner, L. (2007) 'Pre-crime and Post-criminology', *Theoretical Criminology* 11: 261-281.

Zenc (2007) *De toekomst van persoonsinformatiebeleid. Een dynamische kijk op privacy*, Rapport in opdracht van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, The Hague.

Zittrain, J. (2008) *The Future of the Internet. And How to Stop It*, New Haven: Yale University Press.

Zouridis, S. (2000) *Digitale disciplinering. Over ICT, organisatie, wetgeving en het automatiseren van beschikkingen*, Delft: Eburon.

Zureik, E. & M. Salter (eds.) (2005) *Global Surveillance and Policing. Borders, Security, Identity*, Collumpton: Willan Publishing.

Zuurmond, A. (1994) *De infocratie. Een theoretische en empirische heroriëntatie op Weber's ideaaltype in het informatietijdperk,* The Hague: Pheadrus.

Zuurmond, A. & M. Meesters (2005) 'ICT en overheidsorganisatie', pp. 299-327 in M. Lips et al. (eds.) *ICT en openbaar bestuur. Implicaties en uitdagingen van technologische toepassingen voor de overheid*, Utrecht: Lemma.

Zwenne, G.J. (1998) *Belastingheffing en informatieverplichtingen. Reikwijdte en begrenzing van informatiebevoegdheden in de verhouding tussen belastingdienst en banken*, The Hague: Sdu.

Zwenne, G.J., A. Dutler, M. Groothuis, H. Kielman, W. Koelewijn & L. Mommers (eds) (2007) *Eerste fase evaluatie Wet bescherming persoonsgegevens. Literatuuronderzoek en knelpuntenanalyse*, The Hague: WODC.

LIST OF INTERVIEWEES

Positions held at the time of the interview

K. Aarde, Ministry of Justice, Privacy Helpdesk
R. Adams, Rijkswaterstaat
S. Arjun Sharma, Ministry of the Interior and Kingdom Relations
J. Attema, ECP-EPN
M. van Asperdt, National Communications Security Agency
R. Barth, PrivacyBarometer
R.H. van de Beeten, Senator
Prof. V.J.J.M. Bekkers, Professor of ICT Infrastructures in the Public and Private Sector, Erasmus University Rotterdam
A. van Bellen, director of ECP-EPN
B. van den Berg, Tilburg University
L. Beslay, Office of the European Data Protection Supervisor, Brussels
R.O. Blad, Ministry of Economic Affairs
E.Y. Bogerman, director of ICTU
M. Bolhuis, European Privacy Officer for Google Nederland
S. Borgers, CIO for the Ministry of Housing, Spatial Planning and Environment
L. Bos, ICMCC chairman and editor of patientenepd.nl
M. Bouten, ICTU
D. Boyd, Microsoft Research and Harvard University, USA
A.F.M. Brenninkmeijer, National Ombudsman
R. Broekens, consultant at Verdonck Klooster & Associates
Prof. W.A. Brom, Rathenau Institute
I. Brown, Oxford Internet Institute
M. Brugman, ICTU
T. de Bruijn, Permanent Representation of the Netherlands to the EU, Brussels
F. Buijnsters, student and initiator of epd-nee.nl
F. Bussemaker, WCIT2010 Amsterdam program manager
L. Bygrave, University of Oslo
L. Cok, ICTU
N.P. Coleman, Permanent Representation of the Netherlands to the EU, Brussels
O. van Daalen, Bits of Freedom
P. van Dalen, Aliens Police, Brabant Zuid Oost
R. van Dam, CapGemini
N. Damen, project coordinator, Reference Index for Juveniles at Risk (VIR), Ministry for Youth and Family
C. Dekker, GP in Urk and member of the 'Wake up' committee
E.J. Delwel, Dutch Police, programme manager for PROGRIS (information provision in the criminal law chain)

P. Diederen, Advisory Council for Science and Technology Policy (AWT)
J.A. Dijkstra, Netherlands Standardisation Institute (NEN), Electro and ICT business unit
J.W. van Dongen, Personal Records Database and Travel Documents Agency (BPR)
H. Donkhorst, Tax and Customs Administration
E. van Doorn, consultant for Verdonck Klooster & Associates
B. Drewes, information policy coordinator, Association of Dutch Municipalities (VNG)
N. Ducastel, The Expertise Centre
C. van Duijvenvoorden, CIO for the Ministry of General Affairs
J.W. Duijzer, CIO for the Ministry of Agriculture, Nature and Food Quality
Prof. H. van Duivenboden, B&A Consulting/professor of Informatisation and Interorganisational Collaboration, Tilburg University
Prof. S. Dutta, academic director at eLab, INSEAD, Fontainebleau, France
Prof. W. Dutton, director, Oxford Internet Institute
C. Ebbers, privacy consultant
P. van den Eijnden, Ministry of the Interior and Kingdom Relations
S. Eilander, director of Facilities, Accommodation and Purchasing Policy for the Ministry of the Interior and Kingdom Relations
A.C.J.M. Emmaneel, senior policy officer, Data Protection Authority (CBP)
A. van Es, Voelspriet.nl
R van Est, Rathenau Institute
P. van der Feltz, Country Manager for Google Nederland
B. Filippini, PrivacyFirst
J. Flippo, CIO for the Ministry of Foreign Affairs
Prof. H. Franken, Senator/professor of Information Law, Leiden University
E. Frinking, Centre for Strategic Studies
Prof. V.A.J. Frissen, Netherlands Organisation for Applied Scientific Research (TNO)/professor of ICT and Social Change, Erasmus University Rotterdam
H. Gardeniers, director/consultant at Net2Legal privacyadvies
B. Garnier, senior policy adviser on ICT for the Ministry of the Interior and Kingdom Relations
M. van Gelderen, Ministry of Transport, Public Works and Water Management
L. Geluk, executive councillor for Youth, Family and Education, Rotterdam
A. Gerkens, member of the House of Representatives (Socialist Party/SP)
Prof. R. van Gestel, professor of Legislative Drafting Theory and Methodologies, Tilburg University
H. Grevelman, director of Technology and Implementation for SwissLife/member of council of CIOs
H. van Grieken, CapGemini
S. van Grieken, 'Het Nieuwe Stemmen' Foundation
Prof. J.H.A.M. Grijpink, State Councillor for the Ministry of Justice/Utrecht University
M. de Groot, OBA MileStones
F.J. van der Haar, VH Groningen

P. Habets, GP and a member of the Board and vice-chairman of the Dutch Association of General Practitioners (LHV) responsible for ICT
S. van Haersema Buma, member of the House of Representatives (Christian Democrats/CDA)
P. Hagedoorn, partner in 3align Information Governance/Member of Council of CIOs
J. Hakkenberg, director of the Centre for Vehicle Technology (RDW), member of ICTU board of Governors, chairman of the Manifest Group
J. Hamel, Senator
J. van Hattum, Rijkswaterstaat
E. Havenaar, manager, Strategy and External Relations, National IT Institute for Healthcare in the Netherlands (Nictiz)
G. Heimeriks, Advisory Council for Science and Technology Policy (AWT)
M. Heldoorn, policy officer for eHealth, Federation of Patients and Consumer Organisations in the Netherlands (NPCF)
J. Hennis-Plasschaert, member of the House of Representatives (Liberal Party/VVD)
H. Hijmans, Office of the European Data Protection Supervisor, Brussels
Dr. M.W.I. Hillenaar, coordinating CIO, Ministry of the Interior and Kingdom Relations
J. Hoekman, Public Prosecutions Service
S. van der Hof, associate professor, Tilburg Institute for Law, Technology and Society (TILT)
G.-P. van 't Hoff, Multisignaal
V. Homburg, Erasmus University Rotterdam
C.G. van der Hoog, Privacy First
T. Hooghiemstra, The Expertise Centre
Prof. R. Hoppe, professor of Policy Studies, University of Twente
Prof. E. Huizer, director for Knowledge at Netherlands Organisation for Applied Scientific Research (TNO), Professor of Information and Software Systeat Utrecht University
P. Hustinx, European Data Protection Supervisor, Brussels
M. Jaber, ICTU Programme manager for GovUnited
Prof. B.P.F. Jacobs, professor of Software Security and Correctness, Radboud University Nijmegen
R. Jagt, lawyer for ICTU
P. Jansen, policy officer, Dutch College of General Practitioners (NHG)
R. Jansen, ICTU Programme manager for 'eGovernment for citizens'
J.B. de Jong, Ministry of Justice
E. Jongeneel, chain manager for the Safe House in Utrecht
Prof. W. Jonker, Philips Research Europe, professor of Database Technology in Telematics Applications, University of Twente
P. de Kam, senior consultant at The Centre of Expertise (HEC)
N. Kaptein, CapGemini
A. ten Kate-Schoots, lawyer for ICT~Office
S. Katus, Netherlands Railways (NS)
W. Kegel, GBO.Overheid (now Logius)
M.E.M. Kerkvliet, Netherlands Court of Audit

K. Keuzenkamp, deputy director of the Services, Regulatory Burden and Information Policy unit of the Ministry of the Interior and Kingdom Relations
H. Klap, Dutch Police, Cybercrime programme, Board of Chief Commissioners
G. Klei, Privacy helpdesk/OBA MileStones BV
R. Kleijmeer, Netherlands Central Bank (DNB)
T. de Klerk, Rotterdam Metropolitan Area
F. Knopjes, ID Management Centre/Ministry of Justice
E. Koedam, Dutch Police
J. Kohnstamm, chairman, Data Protection Authority
L. Kok, ICTU
B. Kokkeler, senior adviser, Ministry of Agriculture, Nature and Food Quality
H. Kooij, ECID
H.R. Kranenborg, Office of the European Data Protection Supervisor, Brussels
F. Krom, CIO for ING Bank/member of the council of CIOs
N. Kroon, Ministry of Economic Affairs
J. Kuipéri, member of the Executive Board of ICTU
J. Kuipers, Surfnet
F. Kuitenbrouwer, journalist for *NRC Handelsblad* and privacy expert
L. Lap, 'i-Vision' project officer, Ministry of Agriculture, Nature and Food Quality
M. Laqueur, deputy CIO, Ministry of Health, Welfare and Sport
M. Leenaars, Internet Society Nederland
Prof. R.E. Leenes, professor at the Tilburg Institute for Law, Technology and Society (TILT)
L. de Leeuw, Siemans IT Solutions & Services
M. Levering, Identity and Document Fraud Centre of Expertise (ECID)
S. Luijtjens, Shared Service Organisation for Government (GBO)
T.H. van der Maas, deputy director of ECP-EPN
E. Maat, programme director for Innovation and ICT, Ministry of Health, Welfare and Sport
E. MacGillavry, Public Prosecutions Service Research Department
H.C. Maduro, State councillor for the Kingdom of the Netherlands, Council of State
Prof. R. Maes, professor of Information management, University of Amsterdam
Prof. H. Margetts, Oxford Internet Institute
Prof. V. Mayer-Schönberger, Oxford Internet Institute
T. Mekel, director of Business Development and ICT, Athlon Car Lease; Member of the Council of CIOS
Prof. P.L. Meurs, Senator; professor of Healthcare Policy and Managment, Erasmus University Rotterdam
Prof. V. Mitsilegas, professor of European criminal law, Queen Mary University of London
J. Moelker, GBA programme manager for the Ministry of the Interior and Kingdom Relations
J. Moerman, CapGemini
P. Mom, freelance journalist covering eGovernment
L. Mommers, legal intelligence consultant
H. Moraal, Public Prosecutions Service

J. Morijn, Ministry of the Interior and Kingdom Relations
G. Munnichs, Rathenau Institute
R. van Munster, Netherlands Organisation for Applied Scientific Research (TNO), NBF
G.H.M. Nielander, Statistics Netherlands (CBS)
G. van 't Noordende, University of Amsterdam
S. Nouwt, Royal Dutch Medical Association (KNMG)
P. Omtzigt, member of the House of Representatives (Christian Democrats/CDA)
C. van Ooijen, doctoral student, Tilburg Institute for Law, Technology and Society (TILT)
T. van Oosterhout, general project coordinator for the GCOS Information System
M. Oosting, State Councillor for the Kingdom of the Netherlands, Council of State
C. van Oranje, Office of European Commissioner Neelie Kroes (Digital Agenda), Brussels
D. van Oudheusden, Netherlands Central Bank (DNB)
G. Paalman, Sagem Identification
B. Papenhuijzen, CIO for the Ministry of Justice
F. Paul, head of the Large-Scale IT Systeunit, DG Justice, Freedom and Security, European Commission
W. Pedroli, Ministry of the Interior and Kingdom Relations
S. Peereboom, Directorate-General Tax and CustoAdministration, Ministry of Finance
M. Poelmans, Ministry of the Interior and Kingdom Relations
J.K.T. Postma, member of auditcommission of the Dutch civil service
P. Provily, Ministry of Foreign Affairs
M. Raijmakers, Council of State
H. Rauch, principal consultant, CapGemini
P. Reimer, Legal adviser on constitutional affairs, Ministry of the Interior and Kingdom Relations
R. Rinzema, lawyer, Partner Stibbe Advocaten
A.P.C. Roosendaal, doctoral student, Tilburg Institute for Law, Technology and Society (TILT)
H.J.T.M. van Roosmalen, Council of State
R. Roozendaal, CIO for the Ministry of Health, Welfare and Sport
E. Rossieau, Public Prosecutions Service, project secretary for the Cybercrime Intensification Programme
A. Ruifrok, Netherlands Forensic Institute
Prof. M.A. Sasse, professor of Human-Centred Technology, University College London
M. Savelkoul, identity fraud chain manager, Ministry of the Interior and Kingdom Relations
P. van Schelven, lawyer for ICT-Office
A. Schipaanboord, director of policy and innovation, Federation of Patients and Consumer Organisations in the Netherlands, NPCF
R. Schonck, chairman of 'De Vrije Huisarts' Foundation
D. Schravendeel, The Expertise Centre (HEC)
E. Schreuders, director/consultant, Net2Legal privacyadvies
C.J.M. Schuyt, State Councillor for the Kingdom of the Netherlands, Council of State

W. Sijstermans, CIO for the Ministry of Finance
W. van Sluijs, permanent representation of the Netherlands to the EU, Brussels
L.J.E. Smits, director of The Expertise Centre (HEC)
M. Smits, Rathenau Institute
B. Smals, chairman of the board of the Royal Dutch Pharmaceutical Society (KNMP) and pharmacist
Prof. I. Snellen, emeritus professor of Public Administration, Erasmus University Rotterdam
E.-J. Sol, Netherlands Organisation for Applied Scientific Research (TNO)
K. Spaink, columnist/XS4ALL Internet
A. Sprokkereef, visiting researcher at the Tilburg Institute for Law, Technology and Society (TILT)
J. Stam, Ministry of Justice
J. van den Steenhoven, Kennisland
K. van der Steenhoven, CIO for the Ministry of Education, Culture and Science
H. van der Stelt, CIO for the Ministry of Transport, Public Works and Water Management
N. Stolk-Luyten, CIO for the Ministry of the Interior and Kingdom Relations
S. J. Stuiveling, president of the Netherlands Court of Audit
Prof. M. Sturkenboom, professor of Pharmaco-epidemiology, Erasmus University Rotterdam
Prof. K. Stuurman, professor of Information Technology Regulation, Tilburg University; Partner (ICT law) in Van Doorne N.V.
I.Y. Tan, Senator
H. Tankink, deputy director of the Personal Records Database and Travel Documents Agency (BPR)
F. Teeven, member of the House of Representatives (Liberal Party/VVD)
Prof. M. Thaens, The Expertise Centre (HEC)/ROI, professor of ICT and strategic Innovation in the public sector, Erasmus University Rotterdam
C.P. Thissen, Senator
A. Thijssen, director of the Services, Regulatory Burden and Information Policy Unit, Ministry of the Interior and Kingdom Relations
K. Thomeer, GP in Hulst and Medical specialist in Health Information Management in Belgium
M. Timmer, chain manager, Zaanstreek-Waterland Safe House
T. Timmermans, Ministry of the Interior and Kingdom Relations
R. van Troost, Dutch Association for Civil Affairs (NVVB)
J.J.M. Uijlenbroek, director-general of Organisation and Management of Government, Ministry of the Interior and Kingdom Relations
A. Vedder, associate professor at the Tilburg Institute for Law, Technology and Society (TILT)
T. Veenstra, CIO for the Ministry of Economic Affairs
S. in 't Veld, MEP, European Parliament
M.D. van de Velde, project adviser, Identity Fraud Helpdesk, Personal Records Database and Travel Documents Agency (BPR)

W. van Vemde, chief of police, Gooi en Vechtstreek area, responsible for ID, Board of Chief Commissioners
M. Verhagen, deputy director of ICT and application at the Ministry of Economic Affairs
Prof. C. Verhoef, professor of IT Governance, VU University Amsterdam
J. Verschuur, director of ICT Leadership at Ernst & Young
C. Versluis, Social Insurance Bank (SVB)
K. Versmissen, ID-wise
R. Verweij, Institute for the Routing of (Inter)National Information Strea(RINIS)
A. Vlug, design and maintenance manager, National IT Institute for Healthcare in the Netherlands (Nictiz)
G. Vogel, project coordinator for the Electronic Child Dossier (EKD), Twente
G. Wabeke, manager, Lawful Intercept, KPN
P. Waters, head of the Office of the Standardisation Forum
W. Wensink, PriceWaterhouseCoopers
H. Wesseling, CIO at TNT, Member of the Council of CIOs
E. Whitley, London School of Economics
M. Wijnstok, coordinating policy officer, 'i-Vision' project coordinator, Ministry of Agriculture, Nature and Food Quality
P.J. Wijntje, Directorate-general, Tax and CustoAdministration, Ministry of Finance
C. de Wijs, Logica
T. Wijsman, Netherlands Court of Audit
H. Woltring, Zorg Voor Jeugd/Matchpoint
P. van der Zanden, Ministry of Foreign Affairs
D. Zinberg, Harvard University, USA
Prof. A. Zuurmond, professor of ICT and the Future of Public Administration, Delft University of Technology, Partner in Zenc
H. Zwijnenberg, Netherlands Organisation for Applied Scientific Research (TNO)